Luchetta, Giacomo

Conference Paper

The law and economics of intermediaries of personal information

24th European Regional Conference of the International Telecommunications Society (ITS): "Technology, Investment and Uncertainty", Florence, Italy, 20th-23rd October, 2013

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Luchetta, Giacomo (2013) : The law and economics of intermediaries of personal information, 24th European Regional Conference of the International Telecommunications Society (ITS): "Technology, Investment and Uncertainty", Florence, Italy, 20th-23rd October, 2013, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/88481

THE LAW AND ECONOMICS OF INTERMEDIARIES OF PERSONAL INFORMATION

Giacomo Luchetta*

Abstract

This paper explores a class of firms: the intermediaries of personal information. In the economics of personal information, scarcity is no longer the only, and foremost, determinant of value. The most important determinant of value becomes connection. Adapting what Gervais claims to be the first law of an information-flooded cloud-modelled economy, value is not derived from scarcity but rather from the fact that those who value it most will find it. Personal information is the raw material to create connections. Intermediaries collect personal information in exchange for goods or services, regardless of whether they actually need that information to perform their main activity, and use this information to connect other goods and services with the users who value them most, e.g. via personalisation or targeted advertising. Many firms in many different sectors are, or could become, intermediaries of personal information, from Google to supermarkets, from telecom operators to insurance companies.

The descriptive analysis of this industry has consequences in terms of business model and regulatory approach. As for the former, it is worth exploring the conditions for which a firm could profitably become an intermediary of personal information and thereby exploit untapped resources for revenue generation. As for the latter, an imperfect understanding of the economics of personal information creates the risk for misaligned norms, and therefore for an uneven competition.

* PhD Candidate, LUISS "Guido Carli" University, Rome; Researcher, Centre for European Policy Studies, Brussels.

This article greatly benefited from the discussion with Prof. Claudio Feijoo and from comments of Prof. Kristina Irion and Bernardo Rangoni. I also thank the participants to the CEPS Digital Forum Task Force on Online Data Processing in the Context of the EU Data Protection Reform for discussing some of the issues raised in this article.

1 Introduction

I was writing a chapter of my PhD thesis on Google business model when I received a not-so-longed-for letter at home, letting me know that my car insurance was about to expire. So I went to my insurance dealer to hear the ominous amount that I was due to pay. I weakly resisted the quasi-robbery by renouncing to some benefits, and eventually accepted the final deal. Once agreed on the conditions, I had to deliver (or re-confirm) a bulk of personal information to finalise the contract. The reader will be surely familiar with that. Sex, age, place of residence, domicile, brand and model of car, equipments, mileage so far, expected mileage per year and so on and so forth. Then, of course, my insurance company knows even more about me. From my event history, it knows that I use my car both in Brussels and Italy. It knows that I am not a mechanical guy, as I call for the insurance assistance whenever I have a problem, at least when I am not around my hometown. It knows that I am willing to resort to legal actions if needed, as I sued a Belgian insurance for refusing to pay damages. Not all this information is strictly necessary for the insurance company. It is used to pool and segregate risks, to **match** the right premium to my risk profile and my event history. This data allows the insurance company to do a *better*, more tailored and more efficient job.

My insurance company, I realised, is sitting on a mine of personal information which is not fully monetised. That's a pity, as this could be another source of revenues which in turn could maybe, very maybe, lower the price of my car policy. An insurance company could sell targeted ads for mechanic shops, and I would actually appreciate to have a hint about where to go in Brussels in case of problems. It could sell targeted ads for car dealers, knowing which cars I drove so far, my equipments, my mileage and so on and so forth. It could sell targeted ads for insurance-specialised lawyers.[1]

After signing the check, I went home and texted my girlfriend about how much I had to pay, the lack of any meaningful competition in the Italian insurance market, tax increase and so on. My telephone company, had it accessed my SMS, would have acquired a valuable information, which could have used to sell targeted ads to other insurance companies. Had I written an email through my Gmail account rather than an SMS, Google would have accessed that information and actually used to deliver targeted ads. Why such a different use of personal information across companies? Is it only a business model choice? Or are

[1] This paper deals with "positive matching" between users and goods or services. I am aware that the same information could be used to my detriment. E.g., it could be communicated to the Belgian government for registration and tax purposes; or to other insurance companies to raise my premium because I am a legal troublemaker. Still, the focus of this paper is in exploiting matches that create value. How to counter the risk of detrimental matching is a topic worth the same, if not more, attention, but which would take me out of the current research. Having an agnostic stance, in this paper I never intend to argue for a laxer or stricter regulation of personal information, only for a more consistent one.

companies in different sectors regulated differently from the point of view of use of personal information? And which companies are better suited, from a business and regulatory perspective, to profit from personal information, and why?

Begging the reader's pardon for such a digressive introduction, I would like now to provide a more formal map to **the structure of the paper**. The independent variable of this research is the intermediation of personal information. It is claimed that externalities and irrational choice patterns when it comes to privacy may justify the economic regulation of the intermediation of personal information. The "market" for privacy is organised along vertical value chains in which intermediaries of personal information play the pivotal role. The intermediaries operate as retailers of personal information, buying information from users and employing it to match the same users with goods and services. To compare units which are similar from the point of view of how they intermediate personal information, a taxonomy along five dimensions is introduced. Once the "left side" of the logical relation is set, the economic regulation of personal information and privacy, the dependent variable, is brought under the spotlight. This paper aims at answering whether the economic regulation of personal information and privacy is currently treating similar companies in a consistent way or not. I claim that both privacy regulation and competition policy currently neglect the intermediaries of personal information as such, and thereby fail to provide a level playing-field. The same investigation is applied to cloud computing providers, to verify whether the current EU legal framework allows them to become, as predicted, the new class of "dominant" intermediaries.

As shortly sketched above, intermediaries of personal information harvest personal information from users and monetise this information matching users with their own or third-party goods and services. Matching, also called "behavioural targeting" in the online ecosystem,[2] takes place e.g. through personalisation, recommendations,[3] targeted advertising,[4] or dedicated deals. Many firms in many different sectors are intermediaries of personal information. The king is obviously Google with its portfolio of services. Facebook and any social networks are major players too. But many other firms are or at least could be intermediaries of personal information: online sellers, supermarkets offering loyalty programmes, email providers, airlines with or without offering fidelity cards, telecom operators, media companies, financial institutions and insurance companies. They all collect, track, harvest personal information and generate value out of it through matching consumers and producers.

---

[2] CLAUDE CASTELLUCCIA & ARVIND NARAYANAN, EUROPEAN NETWORK AND INFO. SEC. AGENCY, PRIVACY CONSIDERATIONS OF ONLINE BEHAVIOURAL TRACKING (2012).

[3] See Greg Linden, Brent Smith & Jeremy York, Amazon.com recommendations: Item-to-item *collaborative filtering*, 7 IEEE Internet computing 76 (2003).

[4] See OFFICE OF FAIR TRADING, ONLINE TARGETING OF ADVERTISING AND PRICES: A MARKET STUDY (2010).

Raising revenues through matching users and consumers is neither revolutionary nor the only commercial reason to exploit personal information. It has been claimed that firms would have exploited personal information for price discrimination,[5] although this possibility has not materialised so far. For the future, another promising avenue of exploitation seems to be predictive analytics.[6] Other uses include e-commerce safety, or enhanced business processes.[7] Nevertheless, so far matching, especially through targeted ads, is the most widespread way to monetise personal information, and this will be the focus of this paper.

In the current socio-technical environment, matching has become of paramount importance. For intermediaries of personal information, scarcity is no longer the only, or most important, determinant of value. Rather, *connection* is. Adapting what Gervais (2012) claims to be the first law of an information-flooded cloud-modelled economy, *value is not derived from scarcity but rather from the fact that those who value it most will find it*.[8] If this holds, prices, the Hayekian transmitter of information about scarcity, no longer suffice. Connections crate value and personal information is the raw material to create connections.

To be successful, it is no longer necessary for a mechanical shop to be the only one in town able to fix Volkswagen Golfs. The succession of Kondratiev waves made scarcity much less relevant than before. For three centuries space has been undergoing progressive miniaturisation; for at least a century industrial standardization has been becoming the norm; and for the last two decades Internet has been spawning an incredible amount of information, information which can be processed via ubiquitous computers. Uniqueness or scarcity became close to impossible for a vast range of product and services.[9] Rather than upon scarcity, value can be created connecting producers with users, e.g. by letting know all possessors of a Golf that there is a specialized technician nearby. To do so, the technician needs to know who the possessors of a Volkswagen Golf in town are. Personal information creates connections.

---

[5] See Andrew Odlyzko, *Privacy, economics, and price discrimination on the Internet*, *in* ICEC2003: FIFTH INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE 355 (Norman Sadeh ed., 2003).

[6] For a panoramic view of this issue, cf. James Kobielus, The Forrester Wave™: Predictive Analytics And Data Mining Solutions, Q1 2010 (February 4, 2010), ftp://129.35.224.15/software/kr/data/pdf/forpred.pdf.

[7] See ALESSANDRO ACQUISTI, OECD JOINT WPISP-WPIE ROUNDTABLE, THE ECONOMICS OF PERSONAL DATA AND THE ECONOMICS OF PRIVACY (2010); JOHN ROSE, OLAF REHSE & BJÖRN RÖBER, THE BOS. CONSULTING GRP., THE VALUE OF OUR DIGITAL IDENTITY (2012).

[8] Daniel Gervais, *Copyright, culture and the Cloud*, *in* TRANSNATIONAL CULTURE IN THE INTERNET AGE 31 (Sean A. Pager and Adam Candeub eds., 2012).

[9] Interestingly, in the developing economies, where these three factors have not played the same prominent role, the importance of scarcity would be higher. Being the only mechanic shop in Lusaka able to repair a Volkswagen Golf and possessing the specific spare parts does create value.

Intermediaries are the key actors in the economy of personal information, rightly because they have the capacity to create connectivity.[10] Intermediaries collect personal information in exchange for a good or service, regardless of whether they actually need that information to perform their main activity, and use this information to connect other goods and services with the users who value them most. The connection can take different shapes: it can be Amazon suggestions, Groupon daily mails or Google's targeted ads.

Intermediaries are worth exploring on two levels of analysis: their business model and the economic regulation to which they are subject. As for business model analysis, personal information economics is a possible theory for firm behaviours, and consequently for business strategies (mainly in the online sector, but also for brick and mortar companies). Scarcity and price still lead the markets in many sectors. Scarcity, or uniqueness, push consumers to pay a premium for certain products/services/brands, as Apple masterly does. And many companies conquer market shares through a low-price strategy, Ryanair or H&M to name a couple. Still, personal information-based firms are playing a bigger and bigger role in our economy, and it is therefore a territory worth exploring. Most importantly, it is worth exploring the conditions for which a firm could profitably become an intermediary of personal information and thereby exploit untapped resources for revenue generation. Indeed, one of the most successful low-cost companies, Ryanair, raises revenues also by matching customers with car rentals, suitcase manufacturers, and hotels.

Then, from a law and economics perspective, it is worth exploring the implications for economic regulation. I would claim that an imperfect understanding of the economics of personal information creates the risk for misaligned norms. In particular, I fear that different categories of intermediates currently face different regulatory frameworks, because norms are devised over other parameters. For example, a telecom operator may face more difficulties in accessing its customers' communication compared to Google, although in both cases they are trying to access the same kind of information with similar methods. Besides, as far as competition policy is concerned, "an uneven playing field – allowing one firm to use the information that it sees while blocking others from doing the same thing – crates market power through limiting competition"[11].

Finally, one Section is devoted to those which are predicted to be the most important intermediaries of the near future: providers of cloud computing. As Picker put clearly, cloud providers are the "new web intermediaries at the heart of Web 2.0 hav[ing] access to an enormous datastream about their users."[12] Although I embrace most of his seminal analysis, ads-based model is not the only,

---

[10] See Randal C. Picker, *Online Advertising, Identity and Privacy*, (John M. Olin Law & Econ., Working Paper No. 475, 2009); Gervais, *supra* note 8.

[11] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud* 15 (John M. Olin Law & Econ., Working Paper No. 414, 2008).

[12] *Id.* at 3.

and for some services not the dominant, business model for cloud computing. A closer look to these intermediaries will be a ground for applying the theoretical framework reviewed and constructed earlier in this article.

Before the usual scrolling of the paper chapter-by-chapter, I would like to clarify a last point. First, this is a positive-science descriptive paper. No normative judgments on whether more and deeper harvesting and processing of personal information is or is not desirable should be inferred. I personally have a mixed opinion on that. This position may seem unrealistic, but it is necessary to this first attempt to provide an analysis of this class of firms. Of course, further research will need to relax this assumption, as usual, and integrate the dark side of targeted ads. In any case, the assessment of the consequences due to the unprecedented use of personal information in the age of computer networks deserves much deeper reflections, such as Lessig's[13] or Kang's[14], than my quick walk through existing and possible business models and regulations of intermediaries of personal information.

And now the usual scrolling. Section 2 deals with the microeconomics of personal information. First, the behaviour of consumers in the "market for privacy", i.e. consumers' choices over privacy attributes, is reviewed. Then, the market for intermediation of personal information is described as a value chain in which intermediaries operate as retailers of personal information, buying information from users and employing it to match the same users with goods and services. Section 3 provides a taxonomy of intermediaries along five dimensions. In Section 4 two example of economic regulation of intermediaries of personal information are discussed: whether the regulation of privacy and competition policy in the EU creates a level playing-field. Section 5 assesses the same question with respect to the EU legal privacy legal framework for cloud computing providers. Section 6 briefly concludes.

2 Microeconomics of Personal Information

In this section, the microeconomics of personal information will be explored in some details. Firstly, by reviewing the existing stream of literature, I will discuss how individual decision-makers behave when confronted with choices about disclosure of personal data. It will be shown that individuals are quite erratic in matching preferences and behaviours with respect to personal information. The inconsistencies reported have consequences in terms of the economic analysis of different policies. Then, the market for personal information, i.e. the theoretical framework in which intermediaries operate by collecting and selling information, will be analysed. I try to conceptualise this market without resorting

[13] LARRY LESSIG, CODE V. 2.0 (2006).

[14] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV 1193 (2008).

to a two-sided structure, analogously but what I did to define the relevant market of a specific intermediary, Google.[15]

2.1 The Consumer-Side: Personal Information Decision-Making

The economics of privacy analyses the behaviour of individual decision-makers when choosing whether to disclose or not personal information, and its policy implications.

First, some definitional fuss is required. Privacy is a multidimensional, as privacy protects different aspects of life. Hirshleifer's economic analysis contends that privacy can be split into three elements: secrecy, that is the right to keep information private; autonomy, that is the freedom from societal constrains and observation within one's own sphere; and seclusion, that is the right to be left alone.[16] The extensive legal and philosophical review by Solove juxtaposes three additional aspects to Hirshleifer's ones: limited access to the self; control over personal information; and intimacy.[17] Kang discusses privacy in terms of shielding one's own physical space; preserving one's own ability to make choice; and controlling the processing of information about oneself.[18] This article focuses on the control over personal information, in Solove and Kang's meaning.

Still the right to control over his own personal information not only deals with market-based and thereby voluntary disclosure. It also deals with the limitation of the right of the government or the judicature to access personal information, i.e. to coercive disclosure. The focus is here restricted to voluntary disclosure of personal information. Finally, each legal system must define what information is personal information. For the moment, I do not need to be more specific, and this section refers to all information "about himself" submitted by a user to a private intermediary, regardless of whether they would qualify as personal data under any privacy norm. It is worth mentioning that under EU law, personal information is any piece of information related to an identified or identifiable natural person.[19]

---

[15] Giacomo Luchetta *Is the Google Platform a Two-Sided Market?* (2012), *available at* http://ssrn.com/abstract=2048683.

[16] Jack Hirshleifer, *Privacy: its origin, function, and future*, 9 J. LEGAL STUD. 649 (1980).

[17] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002).

[18] Kang, *supra* note 14.

[19] Directive 95/46, of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2, 1995 O. J. (L 281) 31. Hereinafter, the Privacy Directive. The new Commission proposal for a regulation on data protection changes the definition, possibly enlarging the class of personal information. See *Commmission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, art. 4, COM (2012) 11 final (Jan. 25, 2012). Hereinafter, the new Privacy Regulation.

A review of the economics of privacy needs to start from the contributions of the Chicago school.[20] Triggered from a new privacy statute in the USA, these scholars had a narrow focus on assessing the efficiency and the effectiveness of the individuals' right not to disclose certain information. They concluded that any regulation allowing not to disclose personal information in market transactions is ineffective and inefficient from a societal point of view. Absent legal constraints, rational decision-makers would optimally choose both how much information disclose and how much to invest in information discovery. If only the informational aspect of privacy is taken into account, there is nothing new under the sun. Information lubricates the market,[21] and withholding personal information has no better effects than e.g. allowing sellers to conceal product defects.

Chicagoans' original but narrow framing misses at least two important points. First, individuals do benefit from sharing certain personal information, but full disclosure is not in their best interest. A consumers "will rationally want certain kind of information about themselves to be available to producers", as "the transaction is made more efficient if detailed information about the consumer's tastes is available", but at the same time he would rationally conceal some data, as "he doesn't want the seller to know how much he is willing to pay".[22]

Secondly, and possibly most importantly, if the focus is widened from a single transaction to the whole set of transactions with different counterparts, the analysis leads to very different results. Transaction after transaction, disclosure after disclosure, the individual:

> *loses control of the personal information, and that information multiplies, propagates and persists for unpredictable span of time [...]. Hence, the negative utility coming from future potential misuses of offline personal information is a random shock practically impossible to calculate.*[23]

Through a wit metaphor, disclosing data is signing a blank check: it may never come back to the consumer, or it may come back with an arbitrary low or high figure on it.[24]

Recognising that disclosing personal information in a certain transaction may result in costs for the data subject unrelated to that transaction means that the exchange of personal information is subject to a negative externality. More precisely, companies collecting personal data do not internalise future expected

---

[20] George Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623 (1980). Richard Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405 (1981).

[21] Please remember that in the same decade the seminal articles on asymmetric information had been published.

[22] Hal Varian, *Economic Aspect of Personal Privacy*, *in* INTERNET POLICY AND ECONOMICS: CHALLENGES AND PERSPECTIVES, 101, 104 (William H. Lehr & Lorenzo M. Pupillo eds, 2009).

[23] Alessandro Acquisti, *Privacy and Security of Personal Information*, *in* THE ECONOMICS OF INFORMATION SECURITY 179, 183 (L. Jean Camp & Stephen Lewis eds., 2004).

[24] ACQUISTI, *supra* note 7.

costs borne by individuals.[25] This externality implies that, compared to the societal optimum, individuals may over-disclose information and companies may over-invest in collecting information.

Later contributions which complexify the previous analysis introducing second-best scenarios showed that disclosure of personal information may both increase and decrease overall welfare, depending on the initial conditions. Although the sign of the efficiency effect is unclear, privacy norms will always result in distributional effects.[26]

The likelihood and amount of expected losses for data subjects had been skyrocketed by IT technologies. Personal data are nowadays collected, transferred and searched at a pace which was unthinkable before, creating additional and more dangerous threats to one's own sphere. Namely, IT technologies stretch the possible future state of the worlds along two dimensions: probability and expected damages. We are faced with high-probability negligible-cost risks, such as spam; and high-cost low-probability risks, such as identity theft.[27]

High-cost low-probability risks can induce erratic and "irrational" choice patterns, as demonstrated by behavioural economists in many fields.[28] Numerous authors show indeed that there are inconsistencies between individuals' preferences and actual information disclosure.[29] Acquisti and Gross show that while privacy attitudes matter in the decision to whether to join Facebook or not – but only for the age cohorts and social groups for which

---

[25] Lessig, *supra* note 13; Peter H. Huang, *The Law and Economics of Consumer Privacy Versus Data Mining* (1998), *available at* http://ssrn.com/abstract=94041.

[26] Benjamin E. Hermalin & Michael L. Katz, *Privacy, property rights and efficiency: The economics of privacy as secrecy*, 4 QUANTITATIVE MARKETING AND ECON 209 (2006).

[27] Acquisti, *supra* note 7. See also Ian Brown, *Data protection: the new technical and political environment*, 20 COMPUTERS & L. (2010); LRDP KANTOR, COMPARATIVE STUDY OF DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS (Final Report to the Directorate General for Justice, Freedom and Security of the European Commission, 2010) available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

[28] Cf. DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011).

[29] See Acquisti, *supra* note 23; Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior*, *in* THE ECONOMICS OF INFORMATION SECURITY 165 (L. Jean Camp & Stephen Lewis eds., 2004); Kai-Lung Hui & I. P. L Png, *The Economics of Privacy*, *in* 1 ECONOMICS OF INFORMATION SYSTEMS 471 (Terrence Hendershott ed., 2006); Ramon Compañó & Wainer Lusoli *The Policy Maker's Anguish: regulating personal data behaviour between paradoxes and dilemmas, in* ECONOMICS OF INFORMATION SECURITY AND PRIVACY 169 (Tyler Moore, David Pym & Christos Ioannidis eds., 2010); Bettina Berendt, Oliver Günther & Sarah Spiekermann, *Privacy in e-Commerce: Stated Preferences vs. Actual Behavior*, 48 COMM. ACM 101 (2005); Christina Jolls, *Rationality and Consent in Privacy Law* (2010), *available at* http://www.law.yale.edu/documents/pdf/Faculty/Jolls_RationalityandConsentinPrivacyLaw.pdf.

Facebook is not a must-have platform – the amount of information actually disclosed by Facebook users is uncorrelated with their preferences for privacy.[30]

In general, privacy policies and statements are likely neglected by both privacy-savvy and privacy-reckless consumers. Very small, even nihil, rewards suffice for spurring disclosure. Acquisti and Grossklags identify several reasons to explain inconsistencies, such as: limited information on privacy issues; the complexity to compare certain upfront costs and uncertain future benefits; bounded rationality; psychological biases, in particular limited self-control, hyperbolic discounting and underinsurance.[31] Other inconsistencies noticed in privacy behaviours consist of the endowment effects, significantly stronger than for average goods, non-normal distributions of preferences, and order effects.[32] It is interesting to see how these features match Sunstein and Thaler's criteria to identify when rational actors may fail to take self-maximising decisions; therefore external intervention, such as some form of nudging, may be justified.[33]

Taken the behavioural analysis into account, it is quite difficult to predict the effect of different privacy policies. Acquisti concluded that "the market equilibrium will tend *not* to afford privacy protection to individuals",[34] and this can be a ground for privacy regulation. The empirical analysis shows that the plethora of different privacy policies proposed by social networks make hardly any difference in terms of user behaviours.[35] Certainly, claims that opt-in and opt-out policies make no difference to the user can be rejected.[36] Using the *homo oeconomicus* as the role-model for privacy economics would indeed prevent understanding the much ado about default settings, which indeed spark fire among online companies. For example, while in principle online advertisers do not oppose the Do Not Track IP header – which, in short, prevents websites from tracking user behaviours – they did fiercely oppose Microsoft decision to have Do Not Track on by default on Internet Explorer 10.[37] Had we been rational in

---

30 Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, *in* PET '06 (George Danezis & Philipp Golle eds., 2006).

31 Acquisti and Grosslakgs, *supra* note 29.

32 Alessandro Acquisti, Leslie John & George Loewenstein, *What is privacy worth*? (2009), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf.

33 RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

34 ACQUISTI, *supra* note 7, at 6.

35 Joseph Bonneau and Sören Preisbuch, *The Privacy Jungle: On the Market for Data Protection in Social Networks*, *in* ECONOMICS OF INFORMATION SECURITY AND PRIVACY 121 (Tyler Moore, David Pym & Christos Ioannidis eds., 2010).

36 *Contra* Jeffrey M. Lacker, *The Economics of Financial Privacy: To Opt Out or Opt In?*, 88 FED. RES. BANK RICHMOND ECON. Q. 1 (2002).

37 See Natasha Singer, *Do Not Track? Advertisers Say "Don't Tread on Us"*, N.Y. TIMES, Oct. 13, 2012.

our privacy decisions, online advertisers would not go to war for the default option.

Even assigning property rights on private information to individuals is considered at risk of falling short of ensuring an effective privacy protection, especially if bounded consumers' rationality is accounted for.[38] Indeed, under EU law, personal data are protected by a property rule, in Calabresi and Melamed's sense:[39] the right to data collection and processing can be acquired by the counterpart only upon the user's consent.[40] But even under a property rule, intermediaries face no real constraints in obtaining personal information from users.

Lastly, the economic analysis of privacy norms should not forget that regulation may have an expressive function, regardless of its effectiveness, thereby raising users' awareness about their privacy rights. With respect to this function, one may argue that property rights are more "expressive" than regulatory norms,[41] or, rather the opposite, that a human right-based regime will reduce the push for trading and disclosing personal data.[42] Still, this expressive function of law may have an impact on user attitudes, but no factual relevance has been shown in the literature as far as actual behaviours are concerned.

In conclusion, most users will disclose most information in most cases, adopting no or low privacy protections, regardless of whether this is efficient from a static, dynamic, individual or societal point of view.[43] This is due to both negative externalities and inconsistent behaviours. Both grounds can justify, and consequently should shape, pubic intervention to protect privacy.

---

38 Cf. LESSIG, *supra* note 13; Hui & Png, *supra* note 29; Corien Prins, *Property and Privacy: European Perspectives and the Commodification of our Identity*, in THE FUTURE OF THE PUBLIC DOMAIN: IDENTIFYING THE COMMONS IN INFORMATION LAW 223 (Lucie Guibault & P. Bernt Hugenholtz eds., 2006); Varian, *supra* note 22; Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. R. 1125 (2000); Paul M. Schwartz, *Beyond Lessig Code for Internet Privacy: Cyberspace Filters, Privacy-Control and Fair Information Practices*, 2000 WIS. L. REV. 743(2000).

39 Guido Calabresi & Douglas A. Melamed *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

40 I am not claiming that the EU approach is property-based. Clearly, it is human right- (or dignity-) based. Nevertheless, in the strictest technical meaning, art. 7 of the EU Privacy Directive confers the user a property rule-type of protection for collection and processing of personal data. For a wit account of the similarities between a consent-based or property-based regime, see Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J. L. & TECH. 229 (2004); for the similarities of a property-based regime and the current EU legal framework, see Prins, *supra* note 38.

41 As LESSIG does, *supra* note 13.

42 As Kang & Buchner do, *supra* note 40.

43 Sure, there is a non-determined quota of non-users, i.e. of individuals deciding not to enter into a transaction with the intermediary because of privacy concerns.

2.2 The Supply-Side: the Market Structure for Personal Information

The markets in which intermediaries operate can be framed like a retail value chain, namely retailers of personal information. Intermediaries operate in an upstream market, collecting personal information from users, and in a downstream market, selling "matching" (broadly speaking: ads, suggestions, emails etc.) between the "right" users and goods and services to advertisers.

Users enter into contact, and often into a contract, with the intermediary to obtain goods or services. When this happens, intermediaries acquire users' personal information. In some cases, provision personal information is a *condicio sine qua non* for the performance of the contract. For example, buying books on Amazon requires delivering personal data for registration and about one's own purchase history (as purchases take place). In some cases, users can decide whether submitting some of the data requested. For example, to use Gmail, users have to submit a set of personal information for the registration of a Google account, but can refuse to allow indexation of their email content. Finally, in some cases users are free to choose whether to disclose personal information at all. For example, individuals can shop in supermarkets with or without subscribing to its loyalty programme.

The intermediary offers his goods and services "in exchange" of users' personal information. In some cases, personal information is all that the intermediary asks. E.g. most email providers deliver free services in exchange of access to personal information. In other cases, submission of personal information allows the users to enjoy additional benefits, e.g. frequent flyer programmes, or lower prices, e.g. dedicated discounts in supermarkets.

Whichever benefit is traded for personal information, consumers' data is an asset, sometimes the core asset, owned by the intermediary of personal information.[44] The consumer itself, or more precisely his/her personal information, becomes the product. Indeed, intermediaries bear a cost to harvest personal information. In other words, collection of personal information represents a cost for the intermediary, as the acquisition of any other input would.

Based on the personal information retrieved, intermediaries build user profiles and use them as a mechanism to trigger matching, e.g. via targeted advertisements. Profiling users and connecting them with advertisements can either be done by the intermediary itself, that is "first-party advertising", or be outsourced to specialised firms, such as advertising networks, that is "third-party advertising"; third-party ad networks collect data from several websites and merge them into a single user profile.[45] Delivery of the advertisement can take

---

[44] See ACQUISTI, *supra* note 7.

[45] See FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (FTC Staff Report, 2009); ART. 29 WORKING PARTY, OPINION 2/2010 ON ONLINE BEHAVIOURAL ADVERTISING (June 22, 2010); OFFICE OF FAIR TRADING, *supra* note 4; CASTELLUCCIA & NARAYANAN, *supra* note 2; Howard Beales, *The Value of Behavioral Targeting* (2010), *available at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf. Third-party advertising

place either alongside of the delivery of intermediary's goods and services, e.g. Google search or Facebook, on a dedicated *medium*, such as Groupon emails or supermarket snail mails, or on the *medium* of another entity, such as in the case of advertising networks.

On the downstream market, advertisers can be constructed as buyers of access to personal information-based profiles, which are used to deliver targeted messages. In most cases, personal information does not leave either the intermediary, in case of first-party advertising, or the advertising network, in case of third-party.[46] Advertisers just buy the right to deliver an ad to certain class of profiled users. For example, a mechanic shop can asks Facebook to deliver an ad to all users who like Volkswagen and live in Brussels, but would not know the identities of targeted individuals.

Advertisers can buy ads based on two pricing schemes: cost per impression or cost per click.[47] The former scheme is the most widespread across old media: advertisers pay a fixed price, usually expressed per thousand or million viewers (Cost per Million - CPM), to reach a certain amount of audience. Cost per click (CPC) is typical of online ads. In this case, advertisers pay a price each time a viewer clicks on the ads, thereby accessing the advertiser's premises, i.e. its website. The CPC scheme is replicated, to some extent, also on the offline world. For example, clubs use PRs as a marketing strategy. PRs give potential customers a coupon, which is uniquely signed. The club then pays each PR based on the amount of customers who actually accessed its premise.

The two schemes are not *ex ante* Pareto-superior one to the other for advertisers. Assuming that, regardless of the pricing scheme, the same share of customers accessing the advertiser's premises subsequently enters into a transaction, an advertiser is indifferent when

$$\alpha * CPM = CPC$$

where α is the share of ad viewers accessing the advertiser's premises.

However, the CPC scheme is superior on other dimensions. First of all, it creates information. The advertiser knows exactly and in real time how many targeted viewers acceded its premises, rather than having to estimate α. Therefore, CPC

---

is considered potentially more dangerous for users' privacy. Indeed, in first-party advertising personal information does not ever leave the intermediary; on the contrary in third-party networks data is collected by several websites/publishers and then transferred to the ad platform, which merges it into a single user profile. This user profile is much "deeper" than in case of first-party ads, and mixes information from various sources.

[46] E.g. "For Google's paying customers—its advertisers—the information will be in a black box", Picker, *supra* note 11, at 38. He also rightly points out that if Google disclosed the private information, it would allow the advertiser to reach targeted viewers without passing through it, self-destroying its business model.

[47] See Daniel L. Rubinfeld & James D. Ratliff, *Online Advertising: Defining Relevant Markets*, 6 J. COMPETITION L. & ECON. 653 (2010).

solves, partly, the conundrum for which firms "waste half of the money spent in advertising, but do not know which half".[48] Secondly, risk is shifted from advertisers to the intermediary. If the campaign is unsuccessful, i.e. delivers no additional visitors, under CPM the advertiser bears the full cost, while under CPC the advertiser pays nothing and the intermediary bears the opportunity-cost of missed ad revenues. This in turn creates incentives for the intermediary to ensure that ads are channelled towards the mostly interested viewers,[49] i.e. that *those who value the good or service most will find it.*[50] Under CPC, the advertiser is therefore sure that the intermediary will keep on its promises of looking for the most interested viewers, a promise which, as user profiles are not made public, would be hardly monitorable otherwise.

For these reasons, I will assume that advertisers will opt for CPC when possible, although I am aware that there are specific reasons for which in some cases an advertiser prefers to opt for CPM scheme, e.g. to build brand recognition or in case of widespread consumer goods.[51] Furthermore, as I will try to show in Section 3, CPM is *de facto* the only possible option when buying ads from intermediaries which have only statistical information about their users, rather than punctual individual profiles.

Advertisers' surplus as a function of the number of users does not have a point of maximum, because marginal utility of audience, albeit diminishing, is never negative. Since under CPC the marginal cost to reach an additional user, that is its price, is 0, advertisers' surplus increases indefinitely when the number of viewers increases.[52]

This happens because advertisers do not pay for a certain amount of viewers, but of clicks. Advertisers would buy as many clicks as possible, within their budget, as long as their expected profit per click is higher than the price (and 0 clicks afterwards).[53] For this reason, advertisers enjoy Constant Unidirectional

---

48 John Wanamaker, quoted in Picker, *supra* note 11, at 28.

49 See CASTELLUCCIA & NARAYANAN, *supra* note 2.

50 See Rubinfeld & Ratliff, *supra* note 47.

51 For example, Facebook offers both options. See *Campaign Costs & Budgeting*, FACEBOOK.COM, http://www.facebook.com/help/?page=219791638048948 (last visited Sept. 15, 2012).

52 Formally, Gossen's second law is verified only for x approaching infinity, where is the audience (number of viewers). Gossen's second law states that he ratios of prices and marginal utilities of two goods are equal: $\frac{\partial U_x}{\partial U_y} = \frac{p_x}{p_y}$. In our case, x is the audience (number of viewers) and y is a basket representing all other goods. As p_x=0, for the equation to be verified ∂U_x is to be equal to 0. Nevertheless, the marginal utility of viewers is never nihil, if not approaching the limit to infinity: $\lim_{x \to \infty} (\partial U_x) = 0$.

53 See David Evans, *The Economics of the Online Advertising Industry*, 7 REV. NETWORK ECON. 2 (2008).

Network Externalities based on the numerosity of the audience: the higher the audience, the better.[54]

In other words, the advertisers' demand function for audience is infinitely elastic. This assumption is common in the literature on the economics of advertisement[55] and becomes a key feature of the market under the CPC pricing scheme. Indeed, infinite elasticity of the demand for audience is given by the fact that the demand of click saturates the budget as long as the expected profit per click is higher than the CPC.

3 A taxonomy of Intermediaries

All intermediaries follow a comparable business model. They harvest personal information from users, compile user profiles (either in-house or via outsourcing) and match users' profiles with targeted advertisements. Nevertheless, they are, at first sight, very dissimilar companies, ranging from search engines to supermarkets, from financial institutions to social networks. In this section, I provide some coordinates of a tentative map of the world of intermediaries: a taxonomy which allows comparing entities which are similar as far as the intermediation of personal information is concerned

First of all, intermediaries differ in the relative significance of the matching activity. Groupon gets all of its revenues from matching consumers and dealers. Google search engine gets most of its revenues from advertising,[56] and so does Facebook.[57] LinkedIn is a social network as Facebook, but only 26% of its revenues come from advertising.[58] Television channels may be fully or partially funded by ads, or ads-free (in the latter case, they do not belong to the category of intermediaries). Other intermediaries get much lower revenues, as they basically do intermediation on top of their main business activity, For example, supermarkets get very low revenues directly from ads, because they usually

---

54 Luchetta, *supra* note 15.

55 See Simon P. Anderson & Jean J. Gabszewicz, *The Media and Advertising: A Tale of Two-Sided Markets, in* HANDBOOK OF THE ECONOMICS OF ART AND CULTURE (Victor Ginsburgh & David Throsby eds., 2006); Michael Spence & Bruce Owen, *Television Programming, Monopolistic Competition, and Welfare*, 91 Q. J. OF ECON. 103 (1977).

56 Google Financial Statement for 2011, *available at* http://investor.google.com/financial/2011/tables.html.

57 Kim May-Cutler, *Stats: Facebook Made $9.51 in Ad Revenue Per User Last Year In The U.S. and Canada*, TECH CRUNCH (May 3rd, 2012) http://techcrunch.com/2012/05/03/stats-facebook-made-9-51-in-ad-revenue-per-user-last-year-in-the-u-s-and-canada.

58 Leena Rao, *LinkedIn Beats The Street, Q1 Revenue Up 101 Percent To $188.5M; Net Income Up 140 Percent*, TECH CRUNCH http://techcrunch.com/2012/05/03/linkedin-beats-the-street-q1-revenue-up-101-percent-to-188-5m-net-income-up-140-percent.

deliver internal ads only.[59] It may be useful to broadly identify four categories of intermediary models along this dimension:

1) pure intermediary model: share of revenues from matching activity: 81-100%;
2) significant intermediary model: 51-80%
3) partial intermediary model: 15/20-50%
4) marginal intermediary model: <15/20%.

Another distinction which can be made is between online and offline intermediaries. Online intermediary are facilitated in harvesting and processing personal information, and in real-time matching of visitors and advertisements, but they are not the only relevant category. Off-line intermediaries feature notable examples, such as providers of communication services, financial institutions, old media, and supermarkets. Truly, the relevance of the intermediary model is higher in the online economy. Most offline intermediaries are either marginal or partial intermediaries, with the exception of media.

Intermediaries can collect either statistical or punctual information about their users. Statistical information is typical of old media: by buying a certain newspaper or watching a certain TV programme, I reveal statistical information about myself. Namely, I am more likely to have a certain age, education degree, political orientation, interests and so on and so forth.[60] Punctual information consists of collecting specific data about each user. Both statistical and punctual profiles are used to channel advertisements, although the underlying ad logic is quite different. A hotel in Rome will prefer matching its ad to punctual profiles of individuals travelling to Rome, while producers of mass consumption goods may find efficient to broadcast ads to a large but only statistically profiled audience. Statistical information is usually associated to CPM pricing schemes and allows for different marketing strategies, such as raising brand awareness.

Intermediaries can differ as for the relevance of the personal information to which they have access to their productive process, In general, the literature distinguishes between functional and non-functional information, i.e. between information which is necessary for delivering the good/service and the rest. Information relevance is taken into account in devising data protection policies by several authors.[61] Given the technological and market development, we propose a more granular taxonomy of information into four categories:

1. Information is *non-functional* when it is irrelevant for the good or service that the intermediary delivers. For example, a telephone company could access the content of my SMS, but this information is irrelevant for its task,

[59] In theory, one could measure the additional revenues due to targeted own-promotions through loyalty programmes.

[60] See Picker, supra note 10.

[61] See Kang, *supra* note 14; Alexander Novotny & Sarah Spiekermann, *Personal Information Markets AND Privacy: A New Model to Solve the Controversy* (2012), *available at:* http://www.wu.ac.at/ec/wi2013_pdmarkets_v13.pdf.

that is delivering my SMS to the receiver. The same goes with email content *vis-à-vis* my email provider, or Internet traffic with regards to my Internet Service Provider (ISP).

2. Information is *functional* when it is used by the intermediary to improve the quality of its service. For example, Google search engine uses search history to improve the quality of search results;[62] insurance companies collect as many data as possible for a better pooling; and financial institutions ask for credit history to match the conditions of a loan with its riskiness.

3. Information is *necessary* when the good or service cannot be delivered otherwise. For example, a telephone company needs to know to whom I am sending the SMS; Google search engine needs to know my search query.

4. Finally, for some intermediaries information is itself the object of the transaction, therefore the last category is labelled *information-object*. This is the case of social networks, where the personal information sharing is itself the service offered, rather than an ancillary condition. Belonging to the class of intermediaries of information-object implies that prevents anonymisation is not a viable strategy to protect personal information. A Google search or a phone call can be anonymised; an anonymous social network would be of no use.[63]

Finally, it is worth mentioning that a single intermediary can access one or more classes of information.

Finally, a last distinction should be made between intermediaries having a medium on which carrying out the matching activity, e.g. delivering advertisements, and intermediaries without such a medium. Old media, Google and Facebook can transmit advertisements alongside of their content. Supermarkets, Groupon and telephone companies cannot, and have to create dedicated supports (emails, snail mails, telemarketing etc.) to deliver targeted ads.

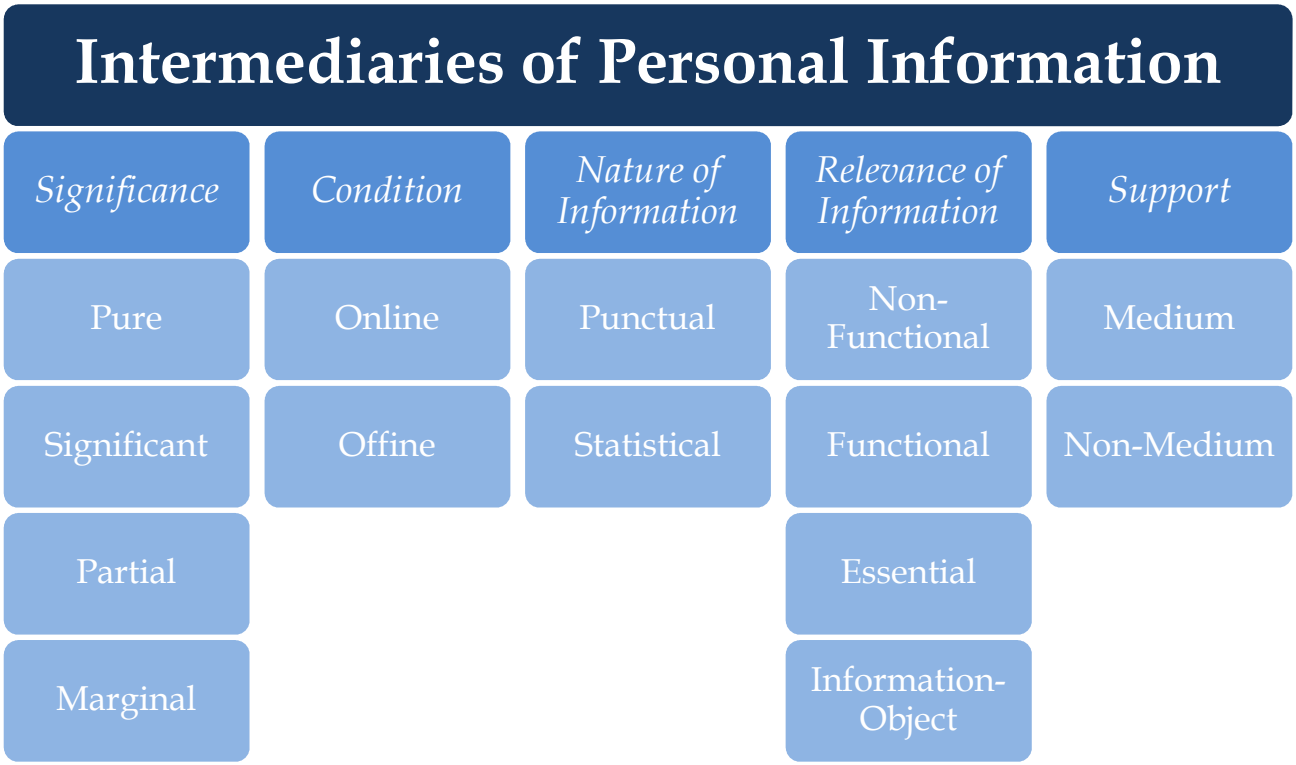
Figure 1 below summarises the typologies of intermediaries.

---

[62] "While search engine providers inevitably collect some personal data about the users of their services, such as IP address, resulting from standard HTTP traffic, it is not necessary to collect additional personal data from individual users in order to be able to perform the service of delivering search results and advertisements." ART. 29 WORKING PARTY ON DATA PROTECTION, OPINION 1/2008 ON DATA PROTECTION ISSUES RELATED TO SEARCH ENGINES (Apr. 4, 2008) 25.

[63] See Picker, supra note 10.

Figure 1 – Taxonomy of Intermediaries



Source: Author's Own Elaboration

The position of the company over these five dimensions is important to develop the intermediary business model in details. First of all, the company should understand whether it can be a pure or marginal intermediary. This depends on business strategies, i.e. whether intermediation is the only activity undertaken or just a way to raise additional revenues from an untapped resource (i.e. from personal information collected for other purposes). The degree of intermediation also depends on the amount of personal information collected: if a company collects personal information at the margin of its activity, such as supermarkets, insurance companies or banks, it will not be in a position to become a pure or significant intermediary. The degree of intermediation also depends on whether the company is brick and mortar only or has an online presence too. In the latter case, it will be easier to directly and indirectly harvest personal information, and the online presence will also provide a channel to deliver ads. If the company has not a medium to deliver ads, it must create one in order to profit from intermediation or sell its information to a medium-endowed company, and that must be addressed *ex ante* in devising the strategy. Finally, consumers are more likely to relinquish personal information when it is necessary or functional to the provision of goods or services. Submission of non-essential information, especially in the offline world, may be resisted as an excessive intrusion of privacy. For example, consumers strongly reacted to the decision of British Telecom to carry out a pilot project for retrieving personal information from

subscribers' Internet traffic,[64] whilst they mind much less when a telephone company reviews our traffic pattern (which is an information necessary for billing) to offer a better tariff plan.

4 Competition and Regulation of Intermediaries

So far we investigated the independent variable of the logical relation between intermediation of personal information and its economic regulation. Namely, we investigated the behaviours of actors in the market for privacy, both consumers and firms, and the proposed a taxonomy to coalesce similar entities. Now, it is time to investigate the dependent variable, that is the economic regulation of intermediaries of personal information. The question is whether economic regulation takes into account the independent variables, i.e. provides a level playing-field to intermediaries which adopt the same business model.[65]

Intermediaries of private information span through different industries. Therefore, they are subject to different sectoral regulations and, for competition law purposes, operate in different relevant markets. I claim that regulation and competition policy have so far overlooked intermediaries of personal information as a group of firms adopting the same business model and therefore competing among each others. Legal analysis has not yet been able to keep the pace with the evolution of business models, especially, but not only, in the online ecosystem.[66]

Currently, firms carrying out the same activity are subject to different norms and constrains. This may put some of them at a disadvantage, up to preventing the implementation of an intermediary business model. In short, some firms can make money by using personal information to raise ad revenues; some others cannot, or can but only at a higher cost. Usually, brick and mortars firms and infrastructure providers are regulated more strictly than online companies.[67] E.g., financial institutions in the US have to obtain users' opt-in content to employ their personal (non-sensitive) information for advertising, and must send a yearly summary of their privacy policies.[68] These requirements are much higher than those imposed on other US companies, such as Google or Facebook.

Below, I provide two more detailed cases, one for regulation and one for competition law. In the former, I try to demonstrate that the same behaviour is regulated differently depending on the type of intermediary, with obvious

---

64 See Andrea N. Person, *Behavioral Advertisement Regulation: How the negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience*, 62 FED. COMMC'N L. J. 435 (2010).

65 See Picker, *supra* note 11.

66 See Andrea Renda, *Neutrality and Diversity in the Internet Ecosystem* (CEPS Digital Forum Academic Papers, 2011), *available at* http://ssrn.com/abstract=1680446.

67 See Picker, *supra* note 11.

68 Financial Services Modernization Act 15 U.S.C. §§ 6801-6809

consequences in terms of the ability to raise ad revenues and therefore on the relative competitive position. In the latter, I try to show how competition policies failed to understand competition mechanisms, and thus to properly define the relevant markets, when dealing with a search engine intermediary such as Google.

4.1 Email scanning vs. Deep Packet Inspection

Most email providers deliver their services for free to consumers.[69] Or, as I tried to argue in this paper, they provide email services as an in-kind payment for users' personal information. Email providers generate revenues from ads and by providing professional services to business customers. Although disaggregated revenue data is not available, as the most widespread providers are part of largest conglomerates, it is fair to consider email providers as pure or significant intermediaries.

Email providers have access to essential, functional and non-functional information. Essential information is e.g. the addressee of my email, or my IP address. Functional information is e.g. the contacts to whom I write most, so that the provider can highlight for me mails from these contacts as "important". Non-functional information is the content of my emails. The providers need not to know what I am writing about, but this can be a precious source of personal information. And two of the three largest web-based email providers,[70] that are Gmail and Yahoo!Mail, scan email content to deliver targeted ads.[71] This is acknowledged in their privacy policies, and an opt-out is offered to users.[72]

Internet Service Providers (ISPs) would be in a comparable position, but it is harder for them to access the data they transmit for intermediation purposes. ISPs sit over a mine of personal information, as whatever we are doing on Internet is conveyed through their "pipes", i.e. their fibre, cable and copper infrastructures. Very few ISPs, unlike email providers, attempted to access non-functional information, that is to observe their subscribers' Internet traffic in some details. This is to some extent surprising, as the depth and breadth of this potential source

---

[69] I chose to compare email providers and telecom operators because of the similarities of their services. The same analysis could be extended, *mutatis mutandis,* to compare tracking cookies and deep packet inspection, as they both aim at tracking browsing behaviours.

[70] Justin Jordan, *Email Client Market Share: New Stats,* LITMUS.COM (June 15, 2012), http://litmus.com/blog/email-client-market-share-stats-infographic-june-2012/email-client-market-share-june-2012.

[71] Hotmail (Microsoft's), the other member of the "big three", pledged not to scan emails content. It delivers targeted ads based only on cookie technologies. See *Privacy Statement,* MICROSOFT.COM (July 2012) http://www.microsoft.com/privacystatement/en-gb/core/default.aspx; Preston Gralla, *Microsoft Bets You're Scared of Google*, COMPUTERWORLD (Apr. 7, 2012), http://blogs.computerworld.com/15898/microsoft_bets_youre_scared_of_google.

[72] See *UK Yahoo! Mail Privacy Statement,* YAHOO.COM http://info.yahoo.com/privacy/uk/yahoo/mail/ymail/; *Google Advertising Privacy Policies*, GOOGLE.COM, http://www.google.com/intl/en/policies/privacy/ads/#toc-personalize.

of personal information makes email content and search queries appallingly smaller.[73]

Real-time access to IP packets as they are travelling on the net is possible via the Deep Packet Inspection (DPI) technology. This technology is actually mandatory for American ISPs, to allow government surveillance of IP traffic for security reasons. On top of that, DPI can be used for network security, network management, and targeted advertising.[74] I will restrain my focus to the latest purpose.

In principle, the mechanism is the same as for email scanning. Both email providers and ISPs wish to access the content of my communication and use this information to match targeted ads. Always in principle, I am entitled to confidentiality both concerning my emails and my Internet traffic. Still, under EU law, the two situations are treated differently.

Art. 5.1 of the ePrivacy Directive[75] requires Member States to ensure confidentiality of communications and the related traffic data, and prohibits surveillance without the user's consent. Email scanning amount to communication surveillance and as such is to undergo user's consent. The issue is what constitutes legitimate consent. Email providers can do so on an opt-out basis: first you get an email address and then, should you wish, you can opt-out from content analysis.

Differently, providers of public communication networks wishing to process traffic data, such as ISPs using DPI technology for advertising purposes, are subject also to art. 6 of the ePrivacy directive. This article prohibits storage of traffic data for non-functional purposes, as long as data are not used to provide value added services. Value added services are defined (sic!) as any service requiring processing of traffic data, thereby the exception covers targeted advertising. Nevertheless, art. 6 exception requires opt-in consent. The failure of the United Kingdom to require opt-in consent for DPI led the European Commission to open an infringement procedure,[76] the most serious legal action that the Commission can undertake against a Member States allegedly non-

---

[73] See Person, *supra* note 64.

[74] See Robert T. G. Collins, *The Privacy Implications of Deep Packet Inspection Technology: why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat*, 44 GA. L. REV. 545 (2010); Angela Daly, *The legality of Deep Packet Inspection*, 14 INT'L J. COMM., L. AND POL'Y (2011).

[75] Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37. Hereinafter, ePrivacy Directie. See also Art. 29 Working Party Opinion 2/2010 *supra* note 45.

[76] Cf. *Telecoms: Commission launches case against UK over privacy and personal data protection,* EUROPA.EU (Apr. 14, 2009), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en.

compliant with a Directive.[77] The United Kingdom later promulgated an act requiring opt-in consent for DPI (OFT 2010), and the infringement procedure was subsequently dismissed.[78]

As it has been argued in Section 2.1, opt-in and opt-out policies are not equivalent, an opt-in policy requires more effort from ISPs and lowers participation rate, thereby reducing collection of personal information and hence ad revenues. Clearly, DPI is quantitatively different from email scanning: more data are harvested from consumers. Still, there is no qualitative difference between the two behaviours. In both cases a communication provider wants to access non-functional confidential information, that is content, to deliver target ads. In both cases, the user is to waive the right of confidentiality to allow access to this information. Why email content is considered less confidential and private than Internet traffic (or SMSs, or voice calls or any other communication service), such as to require opt-in over opt-out, is yet to be fully explained.

4.2 Google vs. Facebook

Competition authorities have considered Google as operating in a two-sided market, whose sides are online advertising and search results.[79] Although the European Commission has not yet cleared this stance, it is also possible that the online advertising market will eventually be split, and that Google relevant markets will be defined as search results and online search advertising.[80] Basically, at least in Europe, Google relevant market will be Google itself.

On the contrary, in the real world Google perceives to have threatening competitors. Surprisingly, it is not about other search engines, but about Facebook. Indeed, they both do money in the same way: collecting personal information and hence matching users and ads. Therefore, they are threats to each other.

Facebook and Google both are intermediaries of personal information. They are very similar along most of the dimensions of intermediation. The share of ad revenues qualifies them as pure intermediaries;[81] they operate online collecting punctual information, and they both have a *medium* to convey ads to the user.

---

[77] See Daly, *supra* note 74.

[78] Cf *Digital Agenda: Commission closes infringement case after UK correctly implements EU rules on privacy in electronic communications,* EUROPEAN COMMISSION (Jan. 26, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/60&type =HTML.

[79] European Commission Decision Case No COMP/M.5727 - Microsoft/Yahoo! Search Business (Feb 2, 2010), at §47.

[80] AUTORITÉ DE LA CONCURRENCE, OPINION NO 10-A-29 ON THE COMPETITIVE OPERATION OF ONLINE ADVERTISING (Dec. 14, 2010), (a non-binding opinion formulated by the French National Competition Authority).

[81] The share of revenues from advertising in 2011 amounts to 96% for Google and 85% for Facebook. Google Financial Statement for 2011, *supra* note 56; U.S. SEC. AND EXCH. COMM'N, FORM S-1 REGISTRATION STATEMENT OF FACEBOOK, INC.

They differ only as to the kind of information collected, as Facebook deals with the information-object type while Google search engine does not.[82]

If competition analysis considered Facebook and Google as intermediaries of personal information, it would emerge clearly that they are fighting in (for?) the same relevant market, something which was already suggested by few authors (Picker 2009; Alexandrov *et al.* 2011; Renda 2011a).[83] In a nutshell,[84] advertisers want to deliver targeted ads based on a large amount of personal information and are likely to consider both Google and Facebook as competing intermediaries.

Competition and regulatory authorities failed so far to grasp the mechanisms of platform completion, which is the main competitive force in the Internet ecosystem. Therefore, they hence failed to ensure regulatory symmetry, in particular pressing on infrastructure providers or software producers, while being looser with over-the-top players, such as content providers (Renda 2011a). Were it acknowledged that many players of the Internet ecosystem are indeed intermediaries of personal information fighting for the same market, competition analysis would become sounder. In particular market definition needs no longer to end up in single-product-markets,[85] and, most importantly, platform competition can finally be taken into proper account as the main explananatory variable of market conducts.

5 Cloud Computing Providers

I continue exploring the logical relationship between intermediation of personal information and its economic regulation by focusing on cloud computing providers. Cloud computing providers are very important actors with respect to intermediation of personal information because it has been predicted that they will be the most important intermediaries of the near future. Cloud providers are the "new web intermediaries at the heart of Web 2.0 hav[ing] access to an enormous datastream about their users."[86]

Cloud computing has already started to change the way in which consumers and firms employ IT technologies. Word processing, data storage, apps development,

---

82 Of course Google+ does, but we focus on the search engine only to keep the case simpler.

83 Picker, *supra* note 10; Alexei Alexandrov, George Deltas and Daniel F. Spulber, *Antitrust and Competition in Two-Sided Markets*, 7 J. COMPETITION L. & ECON 775 (2011).

84 For a more detailed analysis see Luchetta, *supra* note 15.

85 For example, in the competition cases brought about by the Commission against Microsoft, Intel and Google itself. For Microsoft, See Commission Decision Relating to a Proceeding Under Article 82 of the EC Treaty, Case COMP/37.792 (Mar 3, 2004); for Intel, cf. Commission Decision COMP/37.990 Intel (May 13, 2009).

86 Picker, *supra* note 11, at 3.

and many more tasks are, or at least can be, transferred to the cloud. And, according to quasi-unanimous consent, the best has yet to come.

Cloud computing providers are clear candidates to implement the intermediary business model, and several, such as Google's Gmail are. The mine of data to which cloud providers have access is very rich, possibly the richest so far.[87] Indeed, the more our activities will take place in the cloud, the larger datastream we will produce. In perspective, it may be even bigger than traffic data available to ISPs: file storage and document compilation will disclose private information which is currently only marginally conveyed through the Internet.[88] Cloud providers score, across all dimensions, as potentially successful intermediaries: pure and main intermediation has been shown to be a viable strategy in this industry; they may have a *medium* over which ads are conveyed, i.e. the thin cloud client; they operate online; and they have access to punctual information. In addition to that, for the vast majority of cloud providers, this datastream will consist of functional or essential information, i.e. the cloud provider will need to access it to perform its task. This is likely to bring about lower resistance to its harvesting.

Currently, intermediation of personal information, funded via advertising, is not the only, and for some services not the dominant, business model for cloud computing. Therefore it is important to understand whether this is a business strategy or, rather, depends on the privacy legal framework applicable to cloud computing providers.

The importance of cloud providers among the inhabitants of the Internet ecosystem is set to grow. Cloud services are likely to reinforce the tendency for revenues to move into the upper layers of the ecosystem, extracting value from players whose products have been to some extent, commoditised, such as infrastructures and software.[89] Nevertheless, cards are re-shuffling across all layers, since firms from lower layers are becoming cloud providers, such as infrastructure providers, software manufacturers or business service providers. Internet players can build upon their core competences and customer relationships to sell cloud services to users, and in doing so can move from commoditised to higher value layers. E.g. Microsoft is leveraging its Microsoft Office to enter the cloud, IBM and large telecom operators are leveraging their existing business relationships for the same purpose. Such a strategy could be complemented, even boosted, by an ad-funded model for cloud computing. Although I am not sure whether such a scenario is realistic, it would be interesting to see whether a telecom operator could expand into cloud computing

---

87 See Gervais, *supra* note 8; Picker, *supra* note 11, at 3.

88 Picker, *supra* note 11.

89 See Andrea Renda, *Competition, Neutrality and Diversity in the Cloud*, 85 Commc'n. & Strategies 23 (2011).

and harvest personal information up to the point of providing free internet connectivity paid by ads.

The technical and economic framework of cloud computing, which is described in Section 5.1, is quite established by now. On the contrary, the legal framework is still puzzling companies and legal scholars. Crucially, the possibility of implementing the intermediary business model depends on the legal regime applicable to personal data and private information in the cloud. Under EU law, but also in other legal systems, privacy, ownership and use of private information in the cloud are far to be clear, therefore a review of these aspects is provided in Section 5.2.

5.1 Technical and Economic framework

The borders of cloud computing are hard to define. As bluntly put by Larry Ellison, CEO of Oracle, "I can't think of anything that isn't cloud computing with all of these announcements".[90] In some cases, cloud computing includes also what had been previously defined as web 2.0, that is any website with user generated content remotely stored, such as YouTube or Facebook. For sake of this paper, web 2.0 operators are considered as a different category of intermediaries.[91] Under the label cloud computing, in this paper I include firms which deliver IT services on demand, be it software, or hardware tasks such as storage and computational power, over a network.

According to the definition of the US National Institute for Standards and Technology:

> *[c]loud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*[92]

Scholars, whilst adopting different definitions, mostly agree on the main characteristics of cloud computing:[93]

---

[90] Quoted in Jasper P. Sluijs, Pierre Larouche and Wolf Sauter, *Cloud Computing in the EU Policy Sphere* (TILEC Discussion Paper DP 2011-0362011, 2011).

[91] See also Picker, *supra* note 10.

[92] PETER MELL & TIMOTHY GRANCE, NAT'L INST. STANDARDS & TECH., THE NIST DEFINITION OF CLOUD COMPUTING (Special Publication 800-145, Sept 2011), *available at:* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[93] See Gervais, *supra* note 8. David C. Wyld, *The Utility of Cloud Computing as a New Pricing- and Consumption-Model for Information Technology,* 1 INT'L J. DATABASE MANAGEMENT SYS. (2009); C. N. Höfer and Georgios Karagiannis, *Cloud computing services: taxonomy and comparison,* 2 J. OF INTERNET SERV. APPLICATIONS 81 (2011); Renda, *supra* note 89; Christopher S. Yoo, *Cloud Computing: Architectural and Policy Implications*, 38 REV. INDUS. ORG. 405 (2011); Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwiski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica & M. Zaharia, *Above the Clouds: A Berkeley View of Cloud Computing* (UC Berkeley Reliable Adaptive Distributed Systems

1. Virtualisation, that is the possibility of running different and multiple virtual machines over a set of physical infrastructures;
2. Scalability, that is the possibility to allocate hardware resources according to users' needs;
3. Multitenancy, that is the possibility for different users to access the same resources;
4. User configurability;
5. Quality-of-service;
6. Accessibility over the Internet by any device;
7. Pay-per-service.

Although there is disagreement among IT experts,[94] cloud computing providers are usually classified in three categories:

1. Software As A Service: providers of finished applications, such as Google's Gmail or Microsoft's Office 365;
2. Platform As a Service: providers of an environment for developing applications, usually including an operating system, programming languages and other software development tools. E.g. Google's App Engine or Microsoft's Azure.
3. Infrastructure As A Service: providers of hardware resources, such as processing, storage or other computing tasks. E.g. Amazon's EC2, Dropbox.

Potential impacts of cloud computing, once the technology is fully developed, are huge. In a fully cloud-based environment, computing power is transformed in a utility.[95] Firms only have to install "thin" clients, whilst computing power is delivered on demand by large installations, as electricity is. Indeed, Wyld claims that it may represent a change as significant as the electrification of factories.[96] Even before computing fully became a utility, economic impacts of adopting cloud computing are manifold: costs reduction; conversion of IT capital expenditures into operational expenditures, and therefore lower barriers to entry; economies of scale, due to lower unitary cost of processing and storage for mega data centres; aggregation of demand, leading to a higher usage ratio of equipments.[97] Microeconomic impacts and efficiency gains will translate into macroeconomic effects. According to Etro, cloud computing will stimulate economic growth through different channels: increasing business creation and job creation; fostering job reallocation towards more productive sectors; and improving public finance accounts by reducing expenditures and increasing

---

Laboratory, Feb. 10, 2009), *available at*: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

94 *E.g.* Ambrust *et al.*, *supra* note 93.

95 Yoo, *supra* note 93.

96 Wyld, *supra* note 93.

97 See Wyld, *supra* note 93; Höfer and Karagiannis, *supra* note 93; Yoo, *supra* note 93; Sean Marston, Shi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, & Anand Ghalsasi, *Cloud computing — The Business Perspective*, 51 DECISION SUPPORT SYS. 176 (2011); Ambrust, *supra* note 93.

revenues.[98] All in all, cloud computing could increase GDP in the EU by 0.1% to 0.4% per year. For the US, estimates are up to 0.8-1% additional GDP growth per year.[99]

5.2 The legal framework

Under EU law, cloud providers do not benefit from a dedicated legal framework. As information society services, they are covered by the legal framework on e-commerce.[100] Nevertheless, the e-commerce directive aims at ensuring the freedom of providing e-services throughout the Internal Market rather than at comprehensively regulating a class of operators. Namely, it deals with principles such as the freedom of establishment, the applicable jurisdiction, remedies, and with secondary liability. On the contrary, it is not all clear the positioning of cloud computer providers under other EU law branches, that are sectoral regulation and privacy law.

In Europe, sectoral TLC regulation has been tailored over two canonical firms: communication service providers and content providers. Communication service providers undergo a detailed and quite strict regulatory framework, concerning the authorisation regime, access and interoperability of networks, data portability, non-discrimination, universal-service just to name a few.[101] Nevertheless, cloud providers seem to escape the legal definition of communication providers. At the same time, they lack "editorial control", which would qualify them as content providers.[102] Indeed both frameworks would not fit cloud providers. As they do not (yet?) operate an infrastructure which can be qualified as an essential facility, they need not the detailed regulatory framework for communication providers. Still, some of the issues therein regulated, e.g. interoperability or data portability, are relevant for the law and economics of cloud computing as well. For this reason, they are also unlikely to benefit from the looser regulation on content providers. An undefined regulatory framework,

---

98 Federico Etro, *The Economics of Cloud Computing*, 9 The IUP J. Managerial Econ. 7 (2011).

99 Marco Iansiti and Gregory Richards, *Economic Impact of Cloud Computing White Paper* (2011), *available at*: http://ssrn.com/abstract=1875893.

100 Sluijs *et al.*, *supra* note 90. See Directive 2000/31, of the European Parliament and of the Council on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. (L 178) 1.

101 Directive 2002/19, of the European Parliament and Council on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities (Access Directive), 2002 O.J. (L 108) 7; Directive 2002/20, of the European Parliament and of the Council on the Authorisation of Electronic Communications Networks and Services (Authorisation Directive), 2002 O.J. (L 108) 21; Directive 2002/21/EC of the European Parliament and of the Council on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), 2002 O.J. (L 108) 33; Directive 2002/22, of the European Parliament and of the Council on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive), 2002 O.J. (L 108) 51. Commission Directive 2002/77 on Competition in the Markets for Electronic Communications Networks and Services, 2002 O.J. (L 249) 21.

102 Sluijs *et al.*, *supra* note 90.

e.g. on interoperability, could create expectations of vendor lock-in, thereby stifling market take-off.[103]

EU Privacy law[104] finds direct application for cloud providers. Although many scholars discussed the issue and criticised the indeterminacy of a framework which was not thought for cloud computing and could undermine its development,[105] two points seem hard to contest:

1. Cloud providers process data which are "personal" in the meaning of the directive, thereby falling within its scope of applications;[106]
2. Cloud providers, *a fortiori* if generating revenues via targeted ads, are to be considered as data controllers as they, at least in some occasions, determine the means and the purposes of data processing.

The EU privacy law has important implications in terms of i.a. data security, data treatment, data transferability, but it does not prevent a cloud provider to implement an intermediary business model. Everything it needs to do is obtaining consumers' consent to harvest personal information from users' cloud datastream. To a limited extent, email providers are already doing so. Other operators are likely to follow once a critical mass of users, crucial to attract sufficient advertisers because of the Constant Unilateral Network Externalities, switches to cloud-based non-mail services.[107]

It could be questioned, as Reed does,[108] whether the provider has any right of ownership on personal information harvested from data that the user has entrusted to the cloud. Reed argues that data created by the user belongs to the user, while data generated by the operator from data created by the user belongs to the operator. Harvested personal information can be used for revenue-generating activities as long as i) it is not disclosed to third parties without the user's consent; ii) it is not used to compete against the user; or iii) to make profits which could have been made by the user. As long as the re-use of personal information is not concealed and as long as the consumer is arguably enjoying

---

[103] See Paolo Balboni, *Data Protection and Data Security Issues Related to Cloud Computing in the EU*, *in* ISSE 2010 SECURING ELECTRONIC BUSINESS PROCESSES (Norbert Pohlmann, Helmut Reimer & Wolfgang Schneider eds., 2010); Marston *et al.*, *supra* note 97.

[104] Privacy Directive 95/46/EC, *supra* note 19. Directive on e-privacy, *supra* note 75.

[105] *I.a.* Balboni, *supra* note 103; W. Kuan Hon, Christopher Millard & Ian Walden, *The Problem of "Personal Data" in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1* (Queen Mary University of London, School of Law Legal Studies Research Paper No. 75/2011); W. Kuan Hon, Christopher Millard & Ian Walden, *Who is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2* (Queen Mary University of London, School of Law Legal Studies Research Paper No. 77/2011).

[106] The only reasonable exception being the provider of storage-only services requiring users' encryption of data.

[107] DAVID. M. SMITH, GARTNER RESEARCH, THE HYPE CYCLE FOR CLOUD COMPUTING (2011), quoted in Renda, *supra* note 89, at 25.

[108] Chris Reed, *Information "Ownership" in the Cloud* (Queen Mary University of London, School of Law Legal Studies Research Paper No. 45/2010).

lower prices because of the re-use of "his" personal information, *nihil obstat* for the intermediary.

As data harvesting is permitted under privacy law and ownership rights do not prevent cloud providers for making profit out of users' personal information, what happens in the cloud is then a matter of contract law.[109] The terms of reference of the contracts for the provision of services of cloud computing will dictate what cloud intermediaries will or will not be able to do with personal information. Some commentators notice that most privacy policies look like a unilateral appropriation of rights on users' data by cloud intermediary.[110] Some kind of competition over privacy exists, but only for goods and services sold at positive price, while zero-price services showed less of variation over privacy policies.[111] The law and economics analysis would say that data usage rights are not "salient" for consumers, and therefore intermediaries will draft "unfair" terms to appropriate as much surplus as possible (in the framework of Korobkin).[112] On top of that, economics of privacy showed that users' behaviours are not responsive to better privacy policies (cf. Section 2.1). Nevertheless, Microsoft is marketing Office 365 as a privacy friendly cloud service, stating that it will never harvest private information from users' documents. It will be interesting to see whether cloud computing, as e.g. music distribution, will become a battle between brands such as Microsoft and free ad-funded cloud intermediaries.

6 Conclusions

Thanking the reader for coming so far, I would like to point out the reason why this research was undertaken and to summarise its main results. We currently lack a holistic analysis of intermediaries of personal information. They represent the most important class of firms in the online ecosystem, and are important actors also among brick and mortar companies. Still, in many cases legal and economic analysis looks at them through scattered lenses. I have tried to stress that this class of firms is characterised by a similar business model, that is collecting information from users to match users with goods and services. This is how intermediaries generate revenues. This similarity is often neglected because both economic and legal studies focus on the different goods and services that

---

[109] See Gervais, *supra* note 8; William J. Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L. J. 1195 (2010); Reed, *supra* note 108;

[110] *I.a.* Nicole A. Ozer & Chris Conley, *Cloud Computing: Storm Warning for Privacy?* (ACLU of Northern California, Jan. 2010), *available at:* http://www.ntia.doc.gov/files/ntia/comments/100402174-0175-01/attachments/ACLU%20Appendix%20A%20-%20Cloud%20Computing%20Issue%20Paper.pdf.

[111] Sören Preisbuch & Joseph Bonneau, *The privacy landscape: product differentiation on data collection* (2011), *available at*: http://preibusch.de/publications/Preibusch-Bonneau__privacy-landscape.pdf.

[112] Russell B. Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. R. 1203 (2003).

intermediaries provide to users in exchange of personal data, rather than on the data themselves.

To build this framework, it is necessary to start from three main pillars. The first consists of realising that, as Gervais claims,[113] value in the current online ecosystem is built upon connection rather than scarcity. The second consists of understanding the economics of privacy, which explains the micro-behaviour of consumers facing a choice whether to disclose or not personal information. Personal information-intermediaries can exist because, in the current setting, most consumers will disclose most information in most cases; and their business model can thrive because intermediaries can precisely exploit the insights about consumers' privacy choices. Thirdly, the supply side is to be taken into account, acknowledging and framing the business models of intermediaries of personal information. This business model, with some degree of variation, is applied regardless of the goods and services provided to the customers.

Once this framework is laid out, it is possible to cast a taxonomy of personal information-based intermediaries to compare similar entities. Their characteristics vary across five dimensions: i) the share of revenues generated by the intermediating activity; ii) whether they operate online or offline; iii) whether they collect statistical or punctual information; iv) the relevance of the information collected to the business process; v) whether they possess a medium. Depending on where intermediaries are positioned across these five dimensions, they can adopt different strategies to monetise their personal information.

Nevertheless, regulation and competition policy is still blind to the analysis of intermediation of personal information, and regulates intermediaries exclusively based on their sector of activity. It implies that firms which (are willing to) adopt a similar strategy to exploit their data set face different regulations. This is the case illustrated in Section 4.1, where it is shown that e-mail providers and telecom operators cannot process in the same way the same non-functional information (i.e. the content of the communication they convey) in order to deliver targeted ads. As for competition policy, Section 4.2 shows that the failure to analyse the competitive environment in which both Google and Facebook operate leads to skewed results in the definition of the relevant market, and to considering firms facing real competition from other major operators as monopolists. Finally, the analysis of the cloud computing sector showed that whether the intermediary model can be adopted will depend on the legal framework deemed applicable to cloud computing providers.

This is only a first attempt to explore this sector. Further research could profit by proceeding over two directions. First, from an economic point of view, it would be useful to go further in the description of the market for personal intermediaries, modelling them in a more detailed manner than the fresco provided in this paper. Secondly, from a legal point of view, it would be useful to review and assess all the instances in which regulation is not tailored to the

[113] Gervais, *supra* note 8.

personal information business model and creates disparities among different players.