WMG Service Systems Research Group
Working Paper Series

Can You Own Your Personal Data? The HAT (Hub-Of-All-Things) Data Ownership Model

---

Irene CL Ng

ISSN: 2049-4297
Issue Number: 02/18

About WMG Service Systems Group

The Service Systems research group at WMG works in collaboration with industry researching into market design, economic engineering , new business and economic models and value-creating service ecosystems of people, product, service and technology.

The group conducts research that is capable of solving real problems in practice (ie. how and what do do), while also understanding theoretical abstractions from research (ie. why) so that the knowledge results in high-level publications necessary for its transfer across sector and industry. This approach ensures that the knowledge we create is relevant, impactful and grounded in research.

In particular, we pursue the knowledge of digital and data ecosystems design and innovation for value co-creation that is replicable, scalable and transferable so that we can address some of the most difficult challenges faced by businesses, markets and society. The service systems research group operates HATLAB (https://hat-lab.org), the innovation space for the Hub-of-all-Things (HAT) ecosystem.

WMG Service Systems Research Group Working Paper Series
Issue number: 02/18
ISSN: 2049-4297
September 2018

Can You Own Your Personal Data?
The HAT (Hub-Of-All-Things) Data Ownership Model

Ng, Irene CL
Professor of Marketing and Service Systems
Director, HATLAB
Service Systems Research Group
Warwick Manufacturing Group (WMG)
University of Warwick, Coventry, CV4 7AL, UK
Tel: +44 (0) 247652 4871
E-mail address: irene.ng@warwick.ac.uk

Citation:
Ng, Irene C.L. (2018), "Can you own your personal data? The HAT Data Ownership Model", University of Warwick Service Systems Research Group Working Paper series, ISSN 2049-4297 no. 02/18, at ***http://wrap.warwick.ac.uk/108357/***

Can You Own Your Personal Data?
The HAT (Hub-Of-All-Things) Data Ownership Model

This article is an expanded response to the invitation by the Royal Society, the British Academy and TechUK's for the Data Governance seminar on Data ownership, rights and control, 3 October, 2018.

Introduction and background

Research on personal data-sharing in the economics of privacy (e.g. Acquisti 2010 etc.) have found that disclosing personal data do bring benefits to individuals (See Akcura and Srinivasan 2005). However, such sharing also brings about costs and negative externalities, for example, privacy costs, and subjective and objective privacy harms. It has also been suggested that sweeping privacy regulation that result in firms not being able to obtain personal data will lead to opportunity cost and inefficiencies (Acquisti 2010; August and Tunca 2006; Van Zandt 2004; Anderson and de Palma 2005; Hann et al. 2006).

With the increasing economic value of personal data, scholars have been polarised into two main camps. The first, regulatory camp advocates for privacy protection as an end in itself, regardless of economic consequences. The underlying notion of such an advocacy is that privacy is a human right to personal data protection. Yet, even if regulated, enforcement of regulation would be a challenge since there is no statutory authority on the Internet. Any attempt by national governments to enforce privacy regulations would just increase the likelihood of data-driven companies (whose profits depend significantly on data) to employ regulatory arbitrage, moving activities to jurisdictions outside the regulation. The second camp proposes that individuals could be assigned property rights to the information so that they are able to contract with third parties on how they might use it. This self-regulatory framework advocates the exchange of data and data protection to increase aggregate welfare, emphasising market self-correction for efficiency outcomes and the regulators' role as one of steering the market through a combination of incentives, disclosure policies and even liability (Acquisti 2010). Unfortunately, the practical implementation of a self-regulatory framework also faces huge challenges because many of the data exchange contracts are incomplete and there is very little transparency about the secondary uses for the data (Beresford, Kübler, and Preibusch 2010; Godel, Litchfield, and Mantovani 2012). Property rights are a challenge to exercise when the personal data is held by firms collecting the data and not by individuals themselves (Shapiro and Varian, 1997; Laudon 1996). Since personal data is often mixed with other data belonging to the firm, the lack of clear boundaries between personal data and non-personal data within corporate databases would make property rights over personal data within

firms too much of a challenge to implement and enforce. In addition, third parties buying and selling personal data could impose social costs on individuals since individuals are not directly involved in these transactions, resulting in the externalities that are not internalised by the firm (Godel, Litchfield, and Mantovani 2012; Odlyzko 2003; Swire and Litan 1998; Acquisti 2010). All this leads us to conclude that *individuals cannot meaningfully own or control personal data controlled by organisations under current technological systems.*[1]

Coasian economics suggest that it doesn't matter who owns a good, just as long as its ownership – and the boundaries of that ownership – is clear, as a bargaining solution (trade) can emerge. We argue that personal data within organisations cannot meaningfully be "propertised", leading to high transaction costs we currently see. Neither the regulatory nor the self-regulatory initiatives have made much headway in reducing externalities and governments are getting nervous, while consumer groups are demanding action. Some regulation in both the US (California Consumer Privacy Act of 2018[2]) and Europe (GDPR) have increased the access rights of individuals and created legal frameworks for greater excludability. However, the volume of data being used and shared, the opacity of data contracts and regulatory arbitraging, make enforcement a challenge and there is still no evidence on its effectiveness.

Engineering a new set of personal data rights for Individuals

Work in market design through "microeconomic engineering" (Roth 1991) has shown that transactions and institutions matter, and could be redesigned to engender better market outcomes. The challenge is to design a solution for the current situation in personal data that can internalise the current externalities and even reduce them and create more socially efficient outcomes. Evidence from the digital music market have shown that digital music piracy was lowered considerably when music could be downloaded or streamed legally through artist- or licensee-led platforms such as last.fm, Spotify and Apple Music. If an artefact or platform can be economically designed and engineered such that personal data contracts are first party contracts with individuals themselves as both the generator and the contractor of personal data rights, these contracts would be direct and complete between the individual and firms, with less externalities. In addition, if contracted digitally and online, such personal data rights could be available in real time and on demand, such as when a form needs filling or inventory personalised to a set of personal data. If that were possible, then contracts would be complete as individuals could contract whenever needed e.g. with a device such as a mobile phone, without the need for the collecting firm to store it for later use, which

[1] Many organisations claim you own the data they hold. For example, Facebook terms and conditions say explicitly that individuals own their data. However, we argue that ownership is a meaningless concept when individuals do not have the freedom to exercise rights over what they own - I.e. rights to use, exclude (stop someone from using) and transfer (give rights to someone else). In a similar concept to the physical body, individuals can own their bodies, yet may not have any freedom or rights, much like slavery. Ownership without freedom is therefore spurious, and we conclude that personal data held by corporations cannot be meaningfully owned.

[2] https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/

creates uncertainty and incompleteness. Indeed, if such a technological artefact could exist, individuals could even reuse and reshare data acquired from multiple applications for which they generate data (e.g. calendar, hotel bookings) to create better bundled sets of data for re-sharing, resulting in higher social efficiency and improved personal productivity. Finally, the ability to accumulate data through such an artefact could result in better quality multi-source data about the individuals themselves that can potentially be better for an insight and understanding of their health, habits and historical interactions in combination across multiple digital applications and industry siloes, all within the control of individuals, but fully shareable as data rights.

The design of such an artefact is not as straightforward as creating a service to broker personal data. Personal data exist on the Internet under the technological control of multiple apps, websites and services; indeed any user account of an app would have some measure of personal data pertaining to the usage of that app, from sleeping hours to music listens. Any third party service provider who seeks to broker such data would immediately run afoul of intellectual property rights issues. How would such a data broker be any different from current tech giants that already have a lot of personal data, and one can argue, much more incentivised to keep it secure for individuals? The contracting party accessing personal data from the source on the Internet on behalf of individuals e.g. Spotify music listening data, is the data broker itself and therefore the contract is between Spotify and the data broker with the individual's consent. Why would the data broker then be a better broker for the individual than Spotify themselves? Indeed, with increasing data collection abilities of such data brokers, should they exist, the moral hazard and security concerns would rise unless the data brokers become trusts in their own right, protected by some level of guarantee such as regulation, much like lawyers and psychiatrists.

In addition, the reuse and resharing of data rights with others, even with individuals' consent, can become problematic for data brokers because the original rights of the data continue to stay within the source. In other words, if a data broker collected Facebook data on an individual's behalf, the data broker would have to abide by Facebook's terms and conditions for reuse and resharing, even if individuals themselves are willing to contract on. Source data acquired by such data brokers therefore are encumbered and the rights may not be fully vested onto individuals themselves. Since data brokers are trading third party rights, a market for personal data through such a service model is unlikely to work.

Property rights is therefore the most important factor for markets of a good to exist, and personal data as an economic good is no exception, although being in the digital domain, it would fall within the purview of *Intellectual* property rights (IPR) such as patents and copyrights. First party IPR over personal data is important because markets not only enable the exchange of a good, but trade the various exclusive rights associated with the good in terms of its use, exclusion and alienability (Demsetz 1967; Alston, Libecap, and Schneider 1995, Carruthers and Babb 2000).

For individuals to be an active participant in the data economy and to reduce externalities, first party IPR over their data must be economically engineered in some way.

The previous section have concluded that personal data sitting in firms, which I term OPD (organisation-controlled personal data), cannot be sufficiently isolated to grant IPR to individuals, even through data brokers. We propose a first party IPR access model for personal data through the design of a technological artefact, the HAT (Hub-of-All-Things).

Individuals could use the *access* rights mandated by governments (e.g. European General Data Protection Regulation) to claim the data and instead of firm giving rights to individuals for their personal data, firms could be *suppliers* of the same data to individuals if they had the technological ability to hold it. The normal subject access model is to give individuals a file - a PDF or CSV file of their data. Individuals can download the data onto their own PC or devices. Unfortunately, personal data accessed in such a manner are not interoperable nor can they be easily reused and reshared. Individuals can't take their sleeping hours on the 13 September and combine this with their music listening data, for example, and share the data easily. However, the downloaded data does free it from the lien i.e. the rights of that data now sit with the individual as a co-producer of that data, and no longer with the firm. If such OPD access could be executed by a more flexible device that is similar to that of a PC, but one that makes it possible for the individual to reuse and reshare data more easily, first party IPR for personal data could be achieved. Better yet, if OPD access rights are real time and on demand, then there is a greater likelihood a primary market could form as and when contextual opportunities for data contracts emerge.

As it happens, such real time, on demand OPD *access* rights are already partially granted by firms. They are granted to other firms through an interoperable standard access model called "API access", where personal data of one user of an application is shared with another application, with user consent. For example, Spotify grants Sonos speakers access to user's personal data for better combined experiences of listening to Spotify playlists on Sonos speakers. Similarly, personal data from Facebook is shared with Twitter so that users can update their status with the same message. The economic benefit of sharing real time personal data amongst digital applications is to create a network effect and greater lock-in to the services. As long as Fitbit sleep is being used by another application (e.g. MyFitnessPal), the individual will stay loyal to Fitbit to ensure a steady generation of that data for its combined experience.

Given that to be the case, there is no reason why API-based OPD access cannot also be granted to individuals for their own benefit.

Funded through more than £3m RCUK/EPSRC grants, the HAT (Hub-of-All-Things) and its related projects set out to design and engineer a legal, economic and

technological artefact (the HAT Microserver) capable of storing, processing, transforming and exchanging personal data and that also assigns a set of rights to the data to individuals themselves. Its objective is that the personal data sitting within the HAT Microserver can define, sui generis, a new asset class of PPD i.e. person-controlled personal data, the personal data where intellectual property rights and excludability of the data (control) is with individuals. To create the PPD asset class, and the artefact that contains it, the HAT was designed, engineered and built around the following 11 principles derived from the economic properties of data as a digital good:

1. Principle of Co-production Access Rights without lien. Personal data has the axiomatic property of co-production. It is generated through human activity, but collected through technology owned by a firm. The individual must therefore own a technology/device (the HAT Microserver) that is able to collect data in such a way that both the firm and the individual, as co-producers, would have access rights to it in real time and on demand. The data accessed must be free from lien and encumbrances and, subject to prevailing data protection laws, allow both parties to reuse and reshare.

2. Principle of Alienable Rights. Privacy, according to many advocates, should be an inalienable right. Yet the challenge here is not privacy, but that OPD often cannot even be sufficiently isolated to assign rights. While data may not be assigned rights, databases are protected by US copyright law and the EU database directive. Database rights are specifically coded laws on the copying and dissemination of information in computer databases. A database is defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means". Individuals must have their own database and database rights within the HAT Microserver, thereby granting alienable rights for the personal data within, and individuals can grant these rights to others for a period according to their own wishes and for every data point in the database. This must be achieved by the individual executing a set of software code within the HAT Microserver to grant time- and context-dependent exchange of data with low effort. For rights to be assigned without ambiguity, there must also be suitable isolation of each HAT Microserver database from one another. A system of HAT Microservers must therefore be a distributed system of individual HAT Microservers owned by individuals themselves and yet fully interoperable with one another.

3. Principle of Non-rivalrous Consumption. Personal data has an economic property of non-rivalry i.e. consumption of data by an entity does not prevent another entity from consuming it (Shapiro & Varian 1998). This implies that each co-producer may consume the data in a way that benefits itself as well as contract with other parties, without denying the other of consuming and contracting the same. That means API access from data sources into the HAT Microserver database on demand through HAT "data plugs" must create a copy of the data generated but changing the data rights once the data enters the HAT database, so as to ensure that each co-producer has a set of independent rights for the data that sits within their domain.

4. Principle of Expansibility. Personal data has the economic property of infinite expansibility (Rayna, 2008) . That means a firm's data of a person can be copied to another space with very low marginal cost of re-production. The co-producers could hold the same copy of that data in the same instant that it is generated in their respective technological domains/devices, and they have the ability to contract with third parties to continue expanding its use. The HAT schema (data structure) allows infinite combinations of data values across datasets to be exchanged as a data product e.g. Tweets only in Boston, locations between 7-9am. Each of these data values and bundles can be named and then exchanged/contracted through standard APIs using standard Internet protocols and encryption in real time. In a similar way, the firm can do the same with their data (subject to prevailing laws on personal data-sharing).

5. Principle of Excludability. Personal data have an economic non-excludability property, implying that it is near impossible to exclude others from consuming the data unless there is a legal (e.g. contract) or technological (e.g. encryption) framework. Excludability of personal data controlled by individuals must be based on a data contract and/or technological instrument whereby individuals are in a position to grant and/or deny rights over personal data usage. HAT Microservers create data debit contracts when granting rights of HAT data to others and data in transit is SSL-encrypted from end to end, in a similar manner to emails.

6. Principle of Data Derivatives. Personal data have an economic property of recombinant and divisibility (Quah, 2003). Personal data e.g. location, combined with time e.g. 7-9am, can create a secondary, derived data product e.g. commuting journey. A new economic good can be construed as being created when different types of data are combined in such a way that can be exchanged, which means that combining personal data for new exchanges increases the underlying asset value of the database. An individual must control the permission and process of data being combined and transformed (even if it takes seconds) so that the database value increases. The individual must also control the usage of private AI tools on the HAT Microserver that creates new data.

7. Principle of Data as Store of Value. Personal data use contracts cannot specify all states of nature nor all future actions and use of the data, in advance. When there are states or actions that cannot be verified ex post by third parties, they are therefore not contractible ex ante. The literature on incomplete contracts (see Grossman and Hart 1986; Hart and Moore 1990; Aghion and Bolton 1992; Dewatripont and Tirole 1994) have shown that the allocation of power matters when it is not possible to specify in advance precisely how that power should be exercised. Since the value, worth and use of the data is not known, the power to decide on future uncertain contracts must be in the hands of the individual. Therefore, the HAT Microserver has to be the store of value for the individual before a context emerges for an exchange to occur for personalisation or recommendation of products and a data contract emerges. If personal data is available in real time and on demand, every data contract will then be complete for a specific use with no ambiguity and firms have less need to hoard data.

8. Principle of Data as Medium of Exchange. The value of some personal data can expire (perish) if not used e.g. the need for hotel recommendations. It is therefore context and time dependent. Personal data must therefore be available on demand

and in real time to be a superior asset class as well as an effective medium of exchange for data contracts for personalisation and recommendation. By way of the HAT Microserver being a store of value and HAT APIs being the vehicle for exchange, HAT data, in its standardised form, should be treated as currency (like GBP, USD). The only missing element is its ability to be unitised but that can be derived empirically through increase usage, and scale.

9. Principle of Transparency. The way personal data is stored, exchanged and processed and the way it stays at rest, in transit and used must be clear and transparently available for scrutiny. The HAT Microserver must be an open-sourced technology, even if services built on it can be commercial. The processing of data within the HAT must be based on code that is open-sourced and/or standard Internet technologies. The granting of data rights (usage, exclusion and alienability) must be transparent.

10. Principle of Trust Anchoring. Trust is a prerequisite of contracts (Göran and Hägg, 1994). While the HAT Microserver technology has been legally, economically and technically engineered to endow IPR of personal data to individuals, it still needs to be issued like a private data account, much like banks issuing savings or current accounts. For the market to form, HAT Microservers must still be provisioned on license by a trust anchor, which could be the data brokers or data trusts, as long as there are guarantees, either by the state or through market incentives, to stay trustworthy. The difference is that, with IPR resting on individuals, the transferability of data rights can be achieved through a direct and complete contract, much like currency payments, even if it is enabled by data brokers as trust anchors. This would therefore ensure the market viability of data brokers as a service for individuals. Trust anchors could also create additional middleware services or governance mechanisms e.g. hierarchical or nested relationships between HAT owners e.g. parent and child; a power of attorney situation; or create better heuristics of data-sharing practices across apps within the trust anchor's ecosystem.

11. Principle of Market Design. With HAT data having a set of transferable rights, it is now a formal economic good that can create a thin crossing point (Baldwin, 2007) i.e. a transaction boundary for the transfer of rights. Matching of HAT data to apps should be dictated by market design rules of thickness, reduced congestion and safety (Niederle et al., 2008). Best practices of data exchange should be made transparent and allow different types of apps (and different levels of exposures) to play out that will optimise choice and privacy/security concerns.

Implementation

The HAT proof of concept was implemented in November 2016 on AWS (Amazon cloud service) as the first installation while the ability to generate a HAT Microserver (complete with a database) within three seconds of signing up was achieved in July 2017. The implementation of the HAT Microserver was optimised to test its cost structure and a cost of £2 to £4 per month was achieved in January 2018. The HAT is now in live use, both in the innovation environment and in live commercial environment. HATs are open-sourced under AGPL, are portable and can be issued from most devices e.g. HATs in the cloud by different cloud

operators; HATs on a Raspberry Pi or even on a PC at home, or in other devices. However, the security architecture and threat models would differ for each installation, as would the business models. While one person per HAT would disincentivise hacking (a hack of one yields one HAT's data), more work could be done from the security perspective for different types of HAT installations.

Conclusion

The 11 principles of the HAT data ownership model are the basis for the legal, economic and technical engineering of personal data rights for individuals, sui generis, through the HAT Microserver artefact and the re-commodification of personal data into a new asset class for a market to emerge. Containerising individuals' data within their own databases wrapped with microservices allow individuals themselves to be a 'data controller' and 'data processor' for HAT data with low burden of effort. With HAT Microservers, individuals can own their data, and all the rights to it. Open-sourced HAT Microservers can therefore evolve to become the infrastructure for data innovation and AI, to be provisioned by trust anchors. In time, the aspiration is that HAT Microservers become as ubiquitous as PCs and smartphones, artefacts that are personal to individuals.

We argue that the formation of PPD as an asset class can finally emerge a primary market for personal data due to its ability to create differential privacy through selected data (without revealing personal identifying information), bundled multi-source data from the individuals themselves that is verifiable, data that is shareable in real time and on demand from the cloud and that is dynamically accurate, due to individuals themselves being the stakeholders of their data. The HAT Microserver can also install new private AI tools to generate more data from within the Microserver, specifically derivative, higher order and insightful data generated privately from the collection of data within the database; install new plugs to bring more data into the HAT and create data debit contracts with all applications that seek to request for data directly from individuals. Certification of apps are regulated by the HAT Community Foundation and all apps on the HAT have a triple-letter transparent and easy-to-understand rating system for how HAT data is handled by the application.

The HAT Project's ultimate objective is that an explicit, primary market for personal data, similar to the emergence of a primary market for digital music in the early 2000s, would reduce illegal and inefficient personal data markets as well as lessen externalities relating to privacy, as future applications switch to using HATs as user accounts. The HAT model sets up a parallel asset class to challenge the OPD asset class through easier access, higher quality and lower friction, much like the way music licensees challenged music piracy. Hoarding of personal data could also be reduced due to real time availability of data (through APIs) by individuals themselves through their HATs e.g. checking into hotels or filling forms. To date, there are 1400 HAT owners and the platform on Amazon Web Service is live, with 12 pilots that are in various stages of integration with HATs.

References

Acquisti A (2010) The Economics of Personal Data and the Economics of Privacy. Background Paper for OECD Joint WPISP-WPIE Roundtable, 1.

Aghion P, Bolton P (1992) An Incomplete Contracts Approach to Financial Contracting. *The Review of Economic Studies*, 59(3): 473-494.

Alston LJ, Libecap GD, Schneider R (1995) Property Rights and the Preconditions for Markets: The Case of the Amazon Frontier. *Journal of Institutional and Theoretical Economics (JITE) / Zeitschrift Für Die Gesamte Staatswissenschaft* 151(1): 89-107.

Akcura MT, Srinivasan K (2005) Research Note: Customer Intimacy and Cross-Selling Strategy. *Management Science*, 51(6): 1007-1012.

Anderson SP, de Palma A (2005) A Theory of Information Overload. Unpublished manuscript, Department of Economics, University of Virginia. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.487.2261&rep=rep1&type=pdf

August T, Tunca T (2006) Network Software Security and User Incentives.*Management Science,* 52(11): 1703-1720.

Baldwin, C. Y. (2007). Where do transactions come from? Modularity, transactions, and the boundaries of firms. *Industrial and corporate change*, *17*(1), 155-195.

Beresford A, Kübler D, Preibusch S (2010) Unwillingness to Pay for Privacy: A Field Experiment. IZA Discussion Paper No. 5017. .

Carruthers BG, Babb SL (2000) *Economy/society: Markets, Meanings, and the Social Structure*. (Pine Forge Press, Thousand Oaks, CA)

Charter of Fundamental Rights of the European Union, OJ C 364, p. 10, 18.12.2000, Article 8

Demsetz H (1967) Toward a Theory of Property Rights. *American Economic Review*, 57(2): 347-59.

Dewatripont M, s Tirole J (1994) A Theory of Debt and Equity: Diversity of Securities and Manager-Shareholder Congruence. *The Quarterly Journal of Economics*, 109(4): 1027–1054.

Grossman SJ, Hart OD (1986) The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration. *Journal of Political Economy*, 94(4): 691-719.

Godel, M, Litchfield A, Mantovani I (2012) The Value of Personal Information: Evidence from Empirical Economic Studies. *Communications & Strategies*, 88(4th Quarter): 41-60.

Hann IH, Hui KL, Lai YL, Lee TSY, Png IPL (2006) Who Gets Spammed? *Communications of the ACM*, 49(10): 83-87.

Hart OD, Moore J (1990) Property Rights and the Nature of the Firm. *Journal of Political Economy*, 98(6): 1119-1158.

Laudon KC (1996) Markets and Privacy. *Communications of the ACM*, 39 (9): 92-104.

Odlyzko A (2003) Privacy, Economics, and Price Discrimination on the Internet. *Proceedings of the 5th International Conference on Electronic Commerce* (Pittsburgh, Pennsylvania) Sept 3-Oct 3, 355-366. **https://dl.acm.org/citation.cfm?id=948051**

Niederle M, Roth AE, Sonmez. T (2008) Matching and Market Design. Durlauf SN, Blume LE.
The New Palgrave Dictionary of Economics. 2nd Edition.

Quah D (2003) Digital Goods and the New Economy. Chap. 13. Jones DC, ed. *New Economy Handbook* (Elsevier Academic Press, Amsterdam)

Roth AE (1991) Game Theory as a Part of Empirical Economics. *The Economic Journal*, 101, No. 404 (Jan., 1991), pp. 107-114

Shapiro C, Varian HR (1997) US government information policy. Unpublished manuscript, University of California, Berkeley. https://www.researchgate.net/publication/248244291.

Shapiro C, Varian HR (1998) *Information Rules: A Strategic Guide to the Network Economy.* (Harvard Business Press, Boston, MA)

Swire PP, Litan RE (1998) *None Of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive.* (Brookings Institution Press, Washington, D.C.)

Van Zandt T (2004) Information Overload in a Network of Targeted Communication. *The RAND Journal of Economics*, 35(3): 542-560.