The Valuation of Secrecy and the Privacy Multiplier

David Cerezo Sánchez[†]

Calctopia[†]

david@calctopia.com

January 16, 2018

Abstract

How much is secrecy worth and how many times can a secret be sold? This paper introduces a novel method to properly quantify the value of secrecy for the first time and finds that it is supported by empirical evidence. Additionally, it introduces another novel method to model and quantify the Privacy Multiplier, that is, the additional value obtained from the use of privacy-preserving techniques when offering secret data to potentially distrustful third-parties. Altogether, both results close open questions regarding the quantification of the economic impact of the practical application of secure computation technologies, particularly on blockchains.

JEL classification codes: D82, D85, G12, G13

Keywords: valuation, secrecy, privacy, put options, information percolation, rational expectations equilibrium, cryptoeconomics

1 Introduction

Traditionally, the estimation of the value of a secret is based on how much would be lost if the secret was revealed: for example, $500 billion in raw innovation is stolen from U.S. companies each year[Phi13] (i.e., trade secrets, research and development and products that give companies a competitive advantage). This method for valuating secrets exacerbates the already risk-averse judgement[GHM15, HR08] of the secret holder. And since most information is not publicly accesible[Ber01] and intentionally hidden, it's a very natural question to ask for the valuation of secrecy itself.

Withholding information, keeping information secret has an opportunity cost due to the self-imposed restriction on trading said secret information. Therefore, a discount must be applied to the full market value of secret data. This insight forms the basis for the application of advanced techniques from financial valuation to quantify the value of secrecy: this paper uses forward-start put options to upper bound the secrecy discount and price it using the Black-Scholes model, deriving a closed-form formula that is satisfactorily tested on estimations of the valuation of Swiss bank secrecy. This result is useful to estimate how much additional value could be extracted from the vast amounts of data generated and stored each year.

We then study how many times a secret can be sold to different buyers (i.e., the Privacy Multiplier) knowing that the secret will percolate through a network of buyers until it's no longer valuable because it has been incorporated into market prices. Our results provide a concrete, computable model in a rational-expectations equilibrium of the Privacy Multiplier.

Finally, we point out that secure computation technologies can be used to keep information secret while allowing others to use said information: their use compensates the secrecy discount and further multiplies the number of times secret data can be sold, especially in a digital world where the half-life of secrets is declining[Swi15]. These privacy-preserving techniques are indispensable in the setting of permissionless blockchains because they publish all the data of all transactions in the open by default, including the executed smart contracts: private smart contracts give rise to Cryptographically Secure Financial Instruments[Sá15], which benefit their traders and holders by compensating the secrecy discount and applying the Privacy Multiplier.

1.1 Contributions

The main and novel contributions are:

- A new method to value secrecy as a discount on withheld information3.
- A new method to value the Privacy Multiplier4, that is, the additional value obtained when offering data to third-parties with privacy-preserving techniques. And although it's widely acknowledged in cryptographic research that this could be feasible, there are no previous written records of this practice.

2 Related Literature

Previous research has focused on personal and consumer privacy[HK05], not on the value of data as a financial asset:

- Consumer's financial information[Not03] and the implication of opt-in and opt-out policies from the point of view of economic theory and the assignment of property rights.
- The valuation of personal privacy using option privacy theory[BB09b, BB09a].

3 The Secrecy Discount

3.1 Model

A buyer of data that is easily valuable and tradeable at a price P_0 (e.g., customer lists, quotes, and financial series) must keep it secret for a period of time T: consequently, he must be willing to pay a discounted price C for the classified information, lower than P_0. To better accept the deal, a derivative D could be combined with the classified information C such that both would be valued at a higher price than the unrestricted information P_0, the price of the derivative constituting an upper bound for the secrecy discount:

$$C + D \geq P_0 \tag{3.1}$$

In the same way, the buyer could be an owner of data that wants to keep it secret or any other arrangement in which a secrecy discount applies: the restriction to not leak/sell any secret could be self-imposed (e.g., commercial data) or set by an external agent (i.e., classified data from a governmental agency). Additionally, the start date of the derivative D can be chosen at any time t before the expiry date T because the data is secret and the owner is trading on private information: forward-start put options are the best fit for the previously specified derivative, converting to an European put option with the strike price being the forward price of the data at time t and remaining time to maturity $T - t$.

3.2 Assumptions

To ease analysis, a perfect market for the data is assumed:

- Uninterrupted, frictionless trading with no transactions costs and perfectly divisible data.
- Unlimited borrowing and lending at risk-free rate and short selling is allowed.
- Arbitrage is not allowed.

Additionally, there is a risk-free zero-coupon bond B with dynamics

$$dB\left(t\right) = r\left(t\right) B\left(t\right)$$

for an interest rate process $r\left(t\right)$.

3.3 Analytical Upper Bound

The price of a put option with strike price K, maturity date T and spot price P_t is denoted by

$$Pr_t\left(P_t, K, T\right) \tag{3.2}$$

If for every $\epsilon > 0$, the option-pricing function P_t satisfies the following identity

$$\epsilon Pr_t\left(P_t, K, T\right) = Pr_t\left(\epsilon P_t, \epsilon K, T\right) \tag{3.3}$$

then it's said to be homogeneous of degree one regarding the spot price P_t and the strike price K. And by the application of this property, the price of the put option Pr_t to be received when the start date t is known is proportional to the future spot price P_t:

$$Pr_t\left(P_t, P_t e^{\int_t^T r(s)d(s)}.T\right) = P_t \cdot Pr_t\left(1, e^{\int_t^T r(s)d(s)}, T\right) \tag{3.4}$$

The supremum of the put option prices over $[0, T]$ is defined by

$$S_t = \underset{0 \leq r \leq T}{sup} Pr_t\left(1, e^{\int_t^T r(s)d(s)}, T\right) \tag{3.5}$$

The upper bound of the secrecy discount is given by S_t because the holder of the secret data can choose the start time t of the derivative and is unknown to the counterparty, who can hedge the risk by purchasing S_t units of secret data at the issuance date and maintain them until the holder announces the start date t: then, the counterparty must deliver a put option but its current price will less than or equal to the value of S_t units of secret data,

$$Pr_t\left(P_t, P_t e^{\int_t^T r(s)d(s)}, T\right) = P_t \cdot Pr_t\left(1, e^{\int_t^T r(s)d(s)}, T\right) \leq P_t \cdot S_t \tag{3.6}$$

Therefore, the upper bound of the secrecy discount is given by S_T because the price of the put option at the initial time 0 is no larger than $P_0 \cdot S_T$ and the opportunity cost due to the restraint to maintain the secret is precisely given by the price of the forward-start put option with a start date t under the choice of the secret holder.

3.4 Closed-Form Expression

A closed-form expression can be provided for the upper bound on the secrecy discount under the assumption that the spot price follows a time-homogenous process such that

$$Pr_t\left(1, e^{\int_t^T r(s)ds}, T\right) = Pr_0\left(1, e^{\int_0^{T-t} r(s)d(s)}, T - t\right) \tag{3.7}$$

Then, the upper bound on the secrecy discount is given by

$$\begin{aligned} S_T = \underset{0\leq t\leq T}{sup}\, Pr_t\left(1, e^{\int_t^T r(s)d(s)}, T\right) &= \underset{0\leq t\leq T}{sup}\, Pr_0\left(1, e^{\int_0^{T-t} r(s)d(s)}, T-t\right) \\ &= Pr_0\left(1, e^{\int_0^T r(s)d(s)}, T\right) \end{aligned} \tag{3.8}$$

because the price of the put option is an increasing function of the restriction period T (i.e., $T_1 \geq T_2$ implies that $S_{T_1} \geq S_{T_2}$). A closed-form formula for the upper bound on the secrecy discount can be derived from the Black-Scholes model for asset pricing because it's time-homogeneous. Start by assumption that the price of the secret data P_t follows the conventional geometric diffusion process

$$\frac{dP}{P} = (r-y)\, dt + \sigma dW \tag{3.9}$$

where W is a standard Wiener process, r is the constant continuously compounded risk-free rate, y is the constant continuously compounded dividend yield and σ is the constant volatility of the price of the secret data.

The closed-form formula for the secrecy discount is given by

$$S_T = e^{-yT}\left(2\varPhi\left(\frac{\sigma\sqrt{T}}{2}\right) - 1\right) \tag{3.10}$$

as obtained using equation 3.8 on the Black-Scholes price of an European put option with time to maturity T and strike price equal to the forward price $P_0 e^{(r-y)T}$ at time T, and $\varPhi$ is the cumulative normal distribution of mean 0 and standard deviation 1.

3.5 Numerical Interpretation

The following table shows the numerical evaluation of formula 3.10 for volatilities σ ranging from 0.1 to 0.6 and a dividend yield y of 1% as suggested by the paper[CHM15] studying changes in dividend yields from managers' private information:

Period	0.1	0.2	0.3	0.4	0.5	0.6
3 months	1.99%	3.98%	5.96%	**7.95%**	**9.92%**	**11.89%**
6 months	2.81%	5.61%	**8.40%**	**11.19%**	**13.96%**	16.72%
9 months	3.43%	6.85%	**10.26%**	**13.65%**	17.01%	20.35%
1 year	3.95%	**7.89%**	**11.80%**	15.69%	19.54%	23.35%
2 years	5.53%	**11.02%**	16.47%	21.83%	27.09%	32.21%
3 years	6.70%	**13.34%**	19.89%	26.30%	32.51%	38.49%

These estimations of the secrecy discount are in line with the estimations of the valuation of Swiss bank secrecy obtained from a natural experiment in another study[DHZ12]: 8-14% (bolded). Please note that this model should also be valid for valuating trade secrets, but there is not enough empirical data to corroborate this claim[RSV15].

4 The Privacy Multiplier

Definition. The Privacy Multiplier is the additional value obtained from using privacy-preserving techniques (SECCOMP) when offering data to third-parties, denoted by

$$\text{Privacy Multiplier} = \frac{Revenue[SECCOMP = 1]}{Revenue[SECCOMP = 0]}$$

In many cases, secret data can only be sold one time without privacy-preserving techniques (SECCOMP = 0) because the holder exhausts all exclusivity, as in the first-sale doctrine[tUSC76], or it can be sold multiple times but with decreasing prices as the information gets incorporated into the market, depreciating until the information becomes common knowledge. Instead, privacy-preserving techniques (SECCOMP=1) enables multiple sales and contains the depreciation rate.

The concept of the Privacy Multiplier is directly inspired in other multipliers in economics, that is, a factor of proportionality measuring how much an endogenous variable changes in response to a change in some exogenous variable: the misinterpreted money multiplier[CD10], the fiscal multiplier[Kah31] and the Hansen-Samuelson multiplier[Sam39].

4.1 Model

Recent economic studies explicitly model how secret information is generated by market participants, disseminated and finally incorporated into prices:

- Decentralized trading models for over-the-counter markets[GLT09, BK17, Wal16]
- Other models for broker networks[GLT17]

This paper incorporates the model from[AC16] due to its simplicity, although any of the previously listed models could also be used.

Consider an rational-expectation economy[GS80] with investors $i \in [0, 1]$ and T trading dates divided in $t = 0, 1, ..., T-1$ with final liquidation date T. There is a risky security with an unobservable payoff U realized on the liquidation date and following a normal distribution with zero mean and precision H. Prior to the first trading session $t = 0$, each investor i obtains a private signal about the asset payoff:

$$z^i = U + \epsilon^i$$

where ϵ^i is distributed normally and independently of U, has zero mean, precision S and is independent of ϵ^k if $k \neq i$.

Information percolation theory[DGM09] is used to describe how information flows at an increasing rate with its precision becoming heterogeneous across agents: infinitesimally small agents meet each other randomly and share their initial signal and other signals received during previous meetings; meetings take place continuously at Poisson arrival times with meeting intensity λ and

$m_t^i - 1$ agents per meeting. Recent studies largely support the model offered by information percolation theory[HM17].

The cross-sectional distribution of the number of additional signals, π_t, equals the number ω_t^i of signals received by each agent i between trading dates $t-1$ and t: this distribution captures the heterogeneity in information precisions introduced by random meetings. The investor maximizes her expected utility of wealth, W_T^i, choosing her position in the risky asset, D_t^i, at each trading date:

$$\max_{D_t^i} \mathbb{E}\left[e^{-\frac{1}{\tau}W_T^i} | F_t^i\right]$$

subject to

$$W_T^i = X^i P_0 + \sum_{t=0}^{T-2} \left[D_t^i \left(P_{t+1} - P_t\right)\right] + D_{T-1}^i \left(U - P_{T-1}\right)$$

where F_t^i denotes the information set of investor i at time t containing private signals and prices as public signals.

The cross-sectional average of the number of additional signals at time t is defined by

$$\Omega_t = \sum_{n \in \mathbb{N}} \pi_t \left(n\right) n$$

Regarding the economy, investors have exponential utility with a common coefficient of absolute risk aversion $1/\tau$, τ denoting the investor's risk tolerance. Trading takes places at times $t = 0, 1, ..., T-1$ and consumption at time $t = T$, when the asset payoff is realized: X^i denotes the quantity of the risky asset endowed to each investor i at time $t = 0$. The aggregate per capita supply of the risky asset at time $t = 0$ is denoted by

$$X_0 = \int_0^1 X^i di$$

and is normally and independently distributed with zero mean and precision φ; the incremental net supply of liquidity traders, X_t, is normally distributed with zero mean and precision $\mathit{\Phi}$. The normalized price signals are denoted by

$$Q_t = U - \frac{1}{\tau S \Omega_t} X_t$$

Theorem. *(Rational-expectations Equilibrium). There exists a partially revealing rational-expectations equilibrium in the T trading session economy on which the price of the risky asset, P_t, for $t = 0, ..., T-1$ is given by*

$$P_t = \frac{K_t - H}{K_t} U - \sum_{j=0}^{t} \frac{1 + \tau^2 S \Omega_j \varphi}{\tau K_T} X_j$$

The individual and average market precisions, K_t^i and K_t, are given by

$$K_t^i = H + \sum_{j=0}^{t} S\omega_j^i + \sum_{j=0}^{t} \tau^2 S^2 \Omega_j^2 \varphi$$

$$K_t = H + \sum_{j=0}^{t} S\Omega_j + \sum_{j=0}^{t} \tau^2 S^2 \Omega_j^2 \varphi$$

and the individual asset demands, D_t^i, is given by

$$D_t^i = \tau K_t^i \left(\mathbb{E}\left[U|F_i^t\right] - P_t\right) = \tau \left(S \sum_{j=0}^{t} \omega_j^i Z_j^i + \tau^2 S^2 \varphi \sum_{j=0}^{t} \Omega_j^2 Q_j - K_t^i P_t \right)$$

The previous theorem enables us to obtain a concrete, computable definition of the Privacy Multiplier:

Corollary. *The Privacy Multiplier of secret data diffused according to information percolation theory in a rational-expectations equilibrium in the T trading session economy is given by*

$$\textit{Privacy Multiplier} = \frac{\sum_{t=0}^{T} \sum_{i} \left(P_t \left[SECCOMP = 1\right] \cdot D_t^i \left[SECCOMP = 1\right]\right)}{\sum_{t=0}^{T} \sum_{i} \left(P_t \left[SECCOMP = 0\right] \cdot D_t^i \left[SECCOMP = 0\right]\right)}$$

where the individual asset demands

$$D_t^i \left[SECCOMP = 1\right] \gg D_t^i \left[SECCOMP = 0\right], (\forall i, t)$$

and the meeting intensity

$$\lambda \left[SECCOMP = 1\right] \gg \lambda \left[SECCOMP = 0\right]$$

and number of agents per meeting

$$m_t^i \left[SECCOMP = 1\right] \gg m_t^i \left[SECCOMP = 0\right], (\forall i, t)$$

4.2 Empirical Study

Studies on insider trading[Ahe15] provide an informative window on how valuable information percolates investor networks until markets incorporate all the relevant information and it loses relevance: the following table summarizes the diffusion of relevant trading information across 183 insider networks collected by the Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) between 2009 and 2013.

	Order in Tip Chain			
Statistic	1	2	3	4
Tippee house value (Median - $1000s)	668.6	724.5	833.7	1072
Tipper house value (Median - $1000s)	811.7	840.1	758.5	1072
Amount invested (Average - $1000s)	4852	2639	1618.6	1726.1
Amount invested (Median - $1000s)	200.4	250.1	280.1	492.7
Gross profit (Average - $1000s)	759.9	1028.9	230.7	1538.1
Gross profit (Median - $1000s)	17.6	36.3	39.5	86
Tip return (Average - %)	46	43.5	29.2	23
Tip return (Median - %)	25.2	27.9	28.2	18.8
Use shares (%)	50.8	56.2	77.1	76.4
Use options (%)	27	23.4	16.8	21.8
Insider volume/total volume (%)	2.8	4.7	2.9	5.4
Time from information to tip (Days)	12.1	9.2	5	0.4
Tipped passed on received day (%)	46.5	62.7	49.5	92.1
Holding period (Average - days)	13.9	16.8	11.3	9.1
Holding period (Median - days)	5.2	7	4	5
Tippee degree centrality	2.9	2.3	2	1.8
Tipper degree centrality	1.8	4.3	5	4.6

Particularly relevant to this work is the decline of trading returns over the tip chain, indicating that the information is being incorporated into the markets: the investments of the initial tippee returns 46% on average and 25.2% on median; by the fourth link and subsequents, the returns have decreased to 23% for the average and 18.8% for the median. Median gross profits rise from $17,600 to $86,000 per tip, but because the median amount invested rises from $200,400 for the first tippee to $492,700 for the fourth and subsequents.

The speed of the flow of the information over the tip chain also increases with time: the original source waits 12.1 days before tipping, 9.2 days the second linked, 5 at the third link and 0.4 days for the fourth and subsequents links. The fraction of tippers who tip the same day that they receive the information is 46.5%, increasing 92.1% in the fourth and subsequent links, implying that the holding period between when the tippee receives the information and the event date declines over time, from an average of 13.9 days to 9.1 days.

Tippers in later links are more central figures, having more information connections and holding more tipping links to all the other insiders, spreading the information to the periphery of the network: in the first link, tippers have 1.8 connections, 4.3 in the second and 4.6 in the fourth and subsequents. Conversely, the tippee's centrality decreases from 2.9 to 1.8.

This empirical data shows the percolation of privileged information through investor networks until it gets incorporated into prices thanks to the investigations conducted by the SEC and the DOD: comparable dynamics of information diffusion could be expected in other law-abiding settings. And discussed on next section5, privacy-preserving techniques could be used to increase the number of times private information is offered to third parties while containing its depreciation.

5 Applications of Secure Computation and Blockchains

This subsection provides a succinct review of modern secure computation technologies: more detailed reviews can be found on these papers[NVF$^+$17, NVA$^+$17, ABPP15].

Secure computation is an active subfield of cryptography research that studies methods for computing functions of private inputs without revealing the inputs themselves hidden, protecting data during outsourced processing or sharing and removing third parties that could be subverted. Secure computation can be done in many ways, using one or a combination of modern encryption techniques that enable computation on encrypted data: multi-party computation (secret sharing, garbled circuits), fully homomorphic encryption (FHE) and oblivious random access machines (ORAM). Each of these technologies has advantages and disadvantages: for example, MPC techniques are faster than homomorphic encryption, but require much more network interaction between the parties.

Special mention deserves another technique, differential privacy: it defends against an adversary that observes the output of statistical queries to a database trying to infer information and compared to the previously mentioned technologies, it can prevent from inferring and learning too much information from the encrypted dataset using indirect queries. Differential privacy usually considers worst-case guarantees, requiring privacy against an adversary who already knows the entire database except for a single row. And although differential privacy is efficient, it also introduces statistical noise to the results of the queries, thus it's constrained to applications using numerical data that tolerates the imprecise results.

For the purpose of this paper, it's almost immediate that secure computation techniques could be used to sell/rent access to secret data without revealing anything about it: this would remove the secrecy discount levied on secret data, automatically increasing its value. What is more, the same information could be sold multiple times to different parties because secret data would not be directly revealed (i.e., the Privacy Multiplier) and that more than justifies the costs associated with the deployment of secure computation technologies. Note that this scenario must be technically solved in practice: for example, the recent case of "Collateral Analytics v. Nationstar Mortgage"[col17] relates to a database provider of real estate information provided to thousands of customers that was fully downloaded by one of them to start a competitor.

Furthermore, we must consider the impact of blockchains[BMC$^+$15, FRS15, FRS16], distributed ledgers that record transactions between two or more parties in a verifiable and permanent way, keeping a continuously growing list of records which are linked. Most blockchains offer a programming language to implement smart contracts, that is, programmable contracts that are executed or enforced by the blockchain, without human interaction: the execution is done publicly, for anyone to review it, but smart contracts could also be executed with secure computation techniques[Sá17, Sá15]. In this way, vast amounts of secret data would surface on blockchains, a setting where it's natural to sell information.

6 Conclusion

We introduce a novel method to properly quantify the value of secrecy, and another novel method to model and quantify the Privacy Multiplier as secret data percolates through a network of investors: we also find empirical support for both methods.

This analysis reinforces the usefulness of secure computation in decentralized settings, now well grounded in economic terms.

References

[ABPP15] David W. Archer, Dan Bogdanov, Benny Pinkas, and Pille Pullonen. Maturity and Performance of Programmable Secure Computation. Cryptology ePrint Archive, Report 2015/1039, 2015. https://eprint.iacr.org/2015/1039.

[AC16] Daniel Andrei and Julien Cujean. Information Percolation, Momentum and Reversal, 2016. https://www.gsb.stanford.edu/sites/gsb/files/updated_paper.pdf.

[Ahe15] Kenneth R. Ahern. Information Networks: Evidence from Illegal Insider Trading Tips, 2015. https://fisher.osu.edu/supplements/10/15846/INFONET.2015.02.12.pdf.

[BB09a] Stefan Berthold and Rainer Böhme. Slides of Valuating Privacy with Option Pricing Theory, 2009. http://www1.inf.tu-dresden.de/~rb21/publications/BB2009_PrivacyOptions_slides.pdf.

[BB09b] Stefan Berthold and Rainer Böhme. Valuating Privacy with Option Pricing Theory, 2009. http://weis09.infosecon.net/files/128/paper128.pdf.

[Ber01] Michael K. Bergman. The Deep Web: Surfacing Hidden Value, 2001. http://dx.doi.org/10.3998/3336451.0007.104.

[BK17] Ana Babus and Péter Kondor. Trading and Information Diffusion in Over-the-Counter Markets, 2017. https://bfi.uchicago.edu/sites/default/files/file_uploads/KONDOR.pdf.

[BMC$^+$15] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, 2015. http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf.

[CD10] Seth B. Carpenter and Selva Demiralp. Money, Reserves, and the Transmission of Monetary Policy: Does the Money Multiplier Exist?, 2010. https://www.federalreserve.gov/pubs/feds/2010/201041/201041pap.pdf.

[CHM15] Amedeo De Cesari and Winifred Huang-Meier. Dividend Changes and Stock Price Informativeness, 2015. https://www.research.manchester.ac.uk/portal/files/23959356/POST-PEER-REVIEW-NON-PUBLISHERS.PDF.

[col17] Collateral Analytics v Nationstar Mortgage, (N.D. Cal., No 18-cv-19), 2017. https://cdn.patentlyo.com/media/2018/01/CollateralAnalyticsComplaint.pdf.

[DGM09] Darrell Duffie, Gaston Giroux, and Gustavo Manso. Information Percolation, 2009. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770313.

[DHZ12] François-Xavier Delaloye, Michel A. Habib, and Alexandre Ziegler. Swiss banking secrecy: the stock market evidence. *Financial Markets and Portfolio Management*, 26(1):143–176, Mar 2012. https://doi.org/10.1007/s11408-011-0178-6.

[FRS15] Pasquale Forte, Diego Romano, and Giovanni Schmid. Beyond Bitcoin - Part I: A critical look at blockchain-based systems. Cryptology ePrint Archive, Report 2015/1164, 2015. https://eprint.iacr.org/2015/1164.

[FRS16] Pasquale Forte, Diego Romano, and Giovanni Schmid. Beyond Bitcoin – Part II: Blockchain-based systems without mining. Cryptology ePrint Archive, Report 2016/747, 2016. https://eprint.iacr.org/2016/747.

[GHM15] Néstor Gandelman and Rubén Hernández-Murillo. Risk Aversion at the Country Level, 2015. https://files.stlouisfed.org/files/htdocs/publications/review/2015/q1/53-66GandelmanHernandez.pdf.

[GLT09] Mikhail Golosov, Guido Lorenzoni, and Aleh Tsyvinski. Decentralized Trading with Private Information, 2009. https://economics.yale.edu/sites/default/files/files/Faculty/Tsyvinski/decentralized-trade2.pdf.

[GLT17] Mikhail Golosov, Guido Lorenzoni, and Aleh Tsyvinski. The Relevance of Broker Networks for Information Diffusion in the Stock Market, 2017. http://w4.stern.nyu.edu/finance/docs/pdfs/Seminars/1701/1701w-Kermani.pdf.

[GS80] Sanford J. Grossman and Joseph E. Stiglitz. On the Impossibility of Informationally Efficient Markets, 1980. http://www-personal.umich.edu/~venky/talks/stiglitz.pdf.

[HK05] Benjamin E. Hermalin and Michael L. Katz. Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy, 2005. https://pdfs.semanticscholar.org/4fa7/37a528faf673478960ebfc48ae2433d36ac1.pdf.

[HM17] Björn Hagströmer and Albert J. Menkveld. A Network Map of Information Percolation, 2017. https://uclouvain.be/cps/ucl/doc/core/documents/ES_Menkveld.pdf.

[HR08] Glenn W. Harrison and E. Elisabet Rutström. Risk Aversion in the Laboratory, 2008. http://static.luiss.it/hey/ambiguity/papers/Harrison_Rutstrom_2008.pdf.

[Kah31] R. F. Kahn. The Relation of Home Investment to Unemployment. *The Economic Journal*, 41(162):173–198, 1931. http://www.jstor.org/stable/2223697.

[Not03] Loretta Nott. Financial Privacy: An Economic Perspective, 2003. https://www.epic.org/privacy/glba/RL31758.pdf.

[NVA$^+$17] Peter S. Nordholt, Nikolaj Volgushev, Mark Abspoel, Meilof Veeningen, Frank Blom, Niek J. Bouman, and Mykola Pechenizkiy. D2.1 State of the Art Analysis of MPC-Based Big Data Analytics, 2017. https://www.soda-project.eu/wp-content/uploads/2017/02/SODA-D2.1-WP2-State-of-the-art.pdf.

[NVF$^+$17] Peter S. Nordholt, Nikolaj Volgushev, Prastudy Fauzi, Claudio Orlandi, Peter Scholl, Mark Simkin, Meilof Veeningen, Niek Bouman, and Berry Schoenmakers. D1.1 State of the Art Analysis of MPC Techniques and Frameworks, 2017. https://www.soda-project.eu/wp-content/uploads/2017/02/SODA-D1.1-WP1-State-of-the-art.pdf.

[Phi13] Joshua Philipp. The Staggering Cost of Economic Espionage Against the US, 2013. https://www.theepochtimes.com/the-staggering-cost-of-economic-espionage-against-the-us_326002.html.

[RSV15] Gavin C. Reid, Nicola Searle, and Saurabh Vishnubhakat. What's It Worth to Keep a Secret?, 2015. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1273&context=dltr.

[Sam39] Paul A. Samuelson. Interactions between the Multiplier Analysis and the Principle of Acceleration. *The Review of Economics and Statistics*, 21(2):75–78, 1939. http://www.jstor.org/stable/1927758.

[Swi15] Peter Swire. The Declining Half-Life of Secrets and the Future of Signals Intelligence, 2015. https://www.newamerica.org/documents/1459/2.24Declining_Half_Life_of_Secrets.pdf.

[Sá15] David Cerezo Sánchez. PCT/IB2015/055776 - Cryptographically Secure Financial Instruments, 2015. https://www.calctopia.com/papers/csfi.pdf.

[Sá17] David Cerezo Sánchez. Raziel: Private and Verifiable Smart Contracts on Blockchains. Cryptology ePrint Archive, Report 2017/878, 2017. https://eprint.iacr.org/2017/878.

[tUSC76] 94th United States Congress. Copyright Law of the United States (Title 17), Chapter 1, 1976. https://www.copyright.gov/title17/92chap1.html#109.

[Wal16] Johan Walden. Trading, Profits, and Volatility in a Dynamic Information Network Model, 2016. http://faculty.haas.berkeley.edu/walden/HaasWebpage/dynamicnetworkswp2.pdf.