12-2019

The information disclosure trilemma: Privacy, attribution and dependency

Ping Fan KE
Singapore Management University, pfke@smu.edu.sg

The Information Disclosure Trilemma: Privacy, Attribution and Dependency

Ping Fan Ke[1]
School of Information Systems, Singapore Management University,
Singapore

ABSTRACT

Information disclosure has been an important mechanism to increase transparency and welfare in various contexts, from rating a restaurant to whistleblowing the wrongdoing of government agencies. Yet, the author often needs to be sacrificed during information disclosure process – an anonymous disclosure will forgo the reputation and compensation whereas an identifiable disclosure will face the threat of retaliation. On the other hand, the adoption of privacy-enhancing technologies (PETs) lessens the tradeoff between privacy and attribution while introducing dependency and potential threats. This study will develop the desirable design principles and possible threats of an information disclosure system, and discuss how the existing designs and technologies could address the design principles.

Keywords: information disclosure, privacy, attribution, dependency, privacy-enhancing technologies, Blockchain, ring signature, witness encryption, design science

INTRODUCTION

Information disclosure has been playing a key role in facilitating business activities by providing private information to relevant decision makers, which is a prerequisite for economic efficiency. For example, consumers could reveal their preference to market researchers so that firms could develop better products and services. In many cases, the information providers are compensated for their effort, however, trading additional private information for the compensation is often required as discussed in the research on privacy calculus (e.g. Dinev and Hart 2006; Hui et al. 2006; Smith et al. 2011). Suppose the consumer who completed the market

[1] Corresponding author. pfke@smu.edu.sg +65 6826 1346

research survey will receive a coupon as a reward. It is possible for the firm to correlate the survey submission and the information providers' identity once the coupon is redeemed.

When the publication contains sensitive information such as medical records or accusation of wrongdoing, anonymous authorship would be useful for maintaining the integrity of the information. A well-known issue in business research on identifiable subjects is the social desirability bias, and the purpose of having double-blind peer review in academic research is also to minimize this kind of bias. Moreover, hiding the author's identity would be crucial to mitigate the threat to retaliation, especially when the disclosed information involves scandals or conspiracies. For example, The Namibian, a daily newspaper publisher, was sued by a lawyer regarding the publication of Panama Papers-related stories that link him to some illegal businesses (Fitzgibbon 2018). Similarly, Edward Snowden, the former CIA employee who disclosed highly classified information regarding global surveillance, has been charged for violating the Espionage Act of 1917 by the United States government.

While it is debatable for the appropriateness of leaking confidential information, researchers may also get into troubles by publishing sensitive reports without any classified information, which is common in the field of cybersecurity. For instance, security news editors Steve Ragan and Dan Goodin were sued by the companies mentioned in the written article for defamation on accusation of software vulnerability (Whittaker 2018). Similarly, a Hong Kong newspaper used the public information of the Chief Executive to disclose the security vulnerability of TransUnion online platform got caught in legal troubles (Sum 2018). Therefore, some authors may opt to publish the work anonymously due to the potential threats.

In fact, the use of pseudonym or pen name is common for authors when facing such a dilemma. Back to a century ago, William Sealy Gosset used the pen name "Student", because of

the restriction from the company's policy, to publish his seminal work on small sample statistics (Student 1908). In the recent years, the most famous publication using a pseudonym would be the Bitcoin whitepaper by "Satoshi Nakamoto" (Nakamoto 2008), whose identity is still a myth.

However, a higher degree of privacy often comes with the cost of lower degree of attribution. A major challenge of pseudonymous publication is that an influential work with a cryptic identity could attract frivolous people to claim for the authorship. For instance, a businessman named Craig Wright has been claiming himself as the author of Bitcoin frequently despite lacking valid proof (Madore 2019). This issue becomes more challenging when the author lost control on the systems that could be used to proof his or her identity. From the previous Bitcoin example, the email account used by "Satoshi Nakamoto" (satoshin@gmx.com) was compromised by a hacker in 2014 (Southurst 2014), which means any message sent after this point of time could not be used for proof of identity even if it is really sent by the actual author. Moreover, some people believe "Satoshi Nakamoto" had passed away already (Kharif 2019), which further complicates the problem of identifying the authorship.

To address the trade-off between privacy and attribution, a centralized agency such as a publisher is often used to facilitate the anonymous information disclosure. In such a case, the author's identity is concealed by the agency, and the disclosed information could be attributed to the author indirectly through the agency. Audience could judge the credibility and offer compensation based on the agency's quality. Apparently, this design has completely solved the problem. Yet, the solution has a strong dependency on the integrity of the agency, which could be compromised due to economic consideration or poor security configuration. Furthermore, the agency may even sell the identity since it is the only entity who can proof the identity of the author. Such an additional dependency on the centralized agency could introduce additional risks.

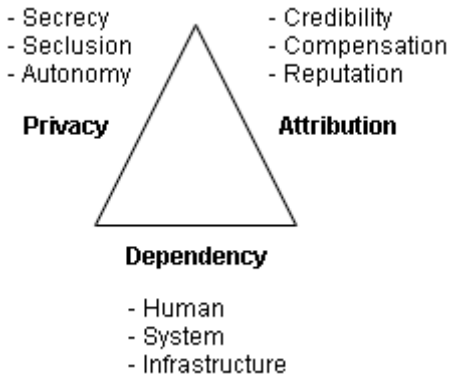

Figure 1. The Information Disclosure Trilemma

In sum, authors who would like to publish anonymously face a trilemma on privacy, attribution and dependency. Without depending on third parties, a privacy-preserving publication can hardly obtain the benefit from attribution; to benefit from attribution, the author needs to be identifiable. Depending on a third party could balance between the two, but with the cost of additional risks and practical feasibility. Nevertheless, the recent development of privacy-enhancing technologies (PETs) like differential privacy and disintermediated systems like Blockchain enable the facilitation of anonymous publication to be depended on technologies rather than single human entity, which is more prone to threats.

In this study, the design principles of building an anonymous publication system, primary for authors who want to publish studies with sensitive information, will be discussed based on a threat model. This research contributes by extending the literature in Cryptoeconomics, which studies the decentralized market using economic theories and applied cryptography, as well as in Bibliometrics with the introduction of new types of authorship metadata.

LITERATURE REVIEW

The current study is directly related to the topic on the anonymity in publications. A notable article published under the pseudonym "Neuroskeptic" discussed the practices and issues of anonymous publications in scientific work, including misconduct exposure and peer review

(Neuroskeptic 2013). They pointed out that anonymous creates a "consequence-free" power, which is necessary in certain situations to provide objective comments. Apart from this benefit, another advantage of anonymous publication is to reduce bias. A commentary work has listed out several biases with revealed identity (Hanel 2015), including the Matthew Effect in science where reputable scholars, universities, countries and journals are more cited after controlling the quality (Merton 1968), the Matilda effect where the contribution of female scientists is attributed to their male colleagues (Rossiter 1993). Therefore, having a proper design on anonymous publication systems is beneficial to scientific research.

Although anonymous publication provides more power to the authors, especially for the science watchdogs, the concern about accountability is significant. Anonymous publications are perceived to be less trustworthy with lower transparency and accountability (Rains 2007). Anonymity also enables Sybil attacks, which could manipulate the review process. For instance, a medicinal-plant researcher named Hyung-In Moon leveraged pseudonymous entities under his control as the reviewers to smoothen the review process of his publications, and many similar cases happened in the past years (Ferguson et al. 2014). How to tackle with the credibility issue in anonymous publication would be an important research question.

More fundamentally, one of the major purposes of having an anonymous publication system is to enable whistleblowing. Prior researches have discussed different facilitating factors of whistleblowing, and a key factor is the statutory protection policy for whistleblower provided by the focal organization (Dixon 2016). However, having an explicit whistle-blowing protection policy, despite appears to be supportive, could discourage potential whistle-blowers since the perceived risk of reporting became more salient (Wainberg and Perreault 2015). Apart from managerial practices, the use of information systems also assists the whistleblowing process, and

research found that anonymity provided by whistleblowing reporting system could increase the willingness to report due to the increase in trust in information quality and report-receiving authority (Lowry et al. 2013). Specifically, the confident that the system will function properly without a backdoor that identifies the reporter is critical to build up the trust. Yet, trust-building is not trivial for such first-party-managed reporting systems. Therefore, the use of PET and decentralized platforms will be discussed in this study.

DESIGN FRAMEWORK

The literature suggests that trust, from both the audience and the author, is a key consideration for building a meaningful anonymous publication ecosystem. Here, the design principles will be derived based on relevant stakeholders in the ecosystem as well as the potential threats to the trust of the mechanism.

System Actors

The essential stakeholder of an anonymous publication system is the author, who produces intellectual works. The author's objectives on privacy and attribution appear to be contradictive, however, could be fulfilled in different period. Like errata, the identity information could be published later for the publication. With this mechanism, the author could be protected from backlash at the first place and be acknowledged when the threat of retaliation is minimal.

A common stakeholder would be the publisher, who will manage the publication process such as quality control and distribution. The publisher may also manage the author's profile as well. Economically speaking, the publisher acts as a platform to maximize the profit from publication activities. Hence, the publisher may breach the author's anonymity when the incentive is not aligned with the author, especially with the presence of principal-agent problem.

Another important stakeholder is the audience, who receives the published information and may react accordingly. As suggested in the literature, a specific interest to the audience is the trustworthiness of the publication, especially with the prevalence of fake news and false information nowadays (Lazer et al. 2018). The author's identity, which is a reputation system by itself, could help audience to assess the quality of the publication. In particular, the author's identity itself would formulate source credibility, and the publication history of the author and the publisher would construct cognitive authority, which influences thoughts (Rieh 2010). When the author is anonymous, audience will rely on other metadata like publisher as preliminary quality assessment before researching on the detail of the content.

In addition, some researchers are interested in studying the statistics regarding authorship on anonymous publications. Typically, this is done by analyzing subtle and unique details embedded in the content of the work, such as Stylometry and Forensic (Holmes 1994, Abbasi and Chen 2005, Stamatatos 2008). To avoid misrepresentation from these side channel analysis, the system could offer a mechanism to verify the author's identity when needed.

On the other hand, some entities accused by the anonymous publication may want to act to the author or publisher. In a less hostile context, the accused party may simply request for the author and the publisher to retract the publication. However, when the alleged party is malevolent, it may use illegal means like stealing the publisher's conversation records to pinpoint the author to take further aggressive actions.

Due to the nature of anonymous publication, opportunists could claim the authorship of published work. In the field of intellectual property right study, a similar behavior is called Copyfraud, where opportunists claim the copyright ownership of the works that are free to everyone like those in the public domain (Mazzone 2006). A subtle difference between the two

frauds is the author of an anonymous publication still owns the copyright of the work due to Berne convention, meaning the author can sue the opportunist for violation of copyright despite proofing the actual authorship will not be trivial.

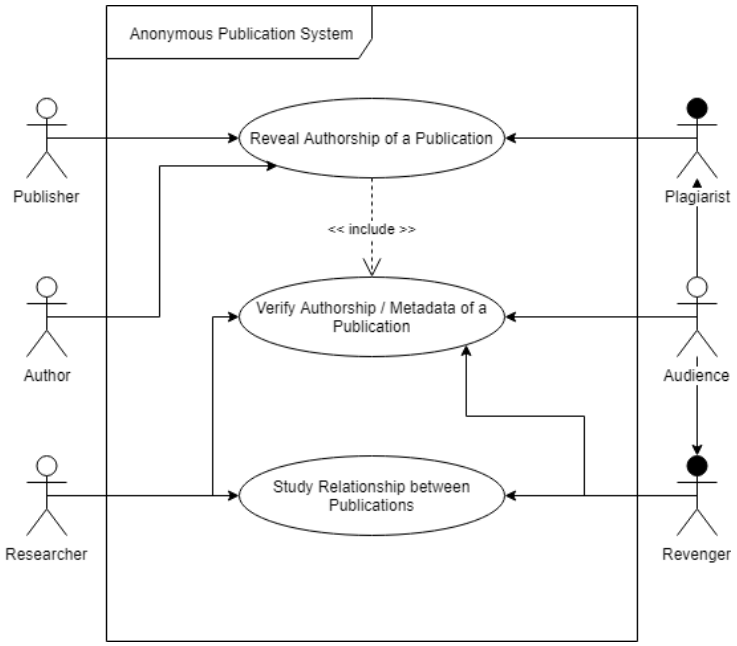

Figure 2. Use Case Diagram

Figure 2 illustrates the primary use (and misuse) cases of an anonymous publication system. A use case that differs from the typically publication system is the revelation of the metadata of a publication, particularly the authorship information. This could be done by the author, the publisher, or opportunists ("Plagiarist"). Another important use case for the general audience is to evaluate the credibility through the metadata, or even the authorship information which are mostly wanted by the alleged entity ("Revenger"). The metadata of a publication also enables researchers to analyze the relationship between publications.

Design Principle

To enumerate the possible threats to the system, the STRIDE threat model which was proposed by Microsoft is adopted (Howard and LeBlanc 2003). STRIDE is an acronym for the

following six categories of threats: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service and **E**levation of Privilege. By considering the potential threats with the system actors, a list of desirable design rules to minimize the threats is derived as shown in Table 1. Table 2 shows the correspondence matrix of these design principles.

Table 1. Design Principle (DP) of Anonymous Publication System

DP1	Except the original author, no other parties should be attributed for the authorship.
DP2	The authenticity of the users in the system should be verifiable by the author.
DP3	The data flow between the author and the publisher should maintain integrity.
DP4	The publisher should be accountable for state changes in the system.
DP5	Only the author could modify access right of the corresponding metadata.
DP6	The authorship metadata should be inaccessible by public by default.
DP7	The system should allow researcher to access certain metadata for analysis purpose.
DP8	The system should provide identity recovery mechanism for the author.
DP9	The system should allow entity-based access control rather than solely group-based.

Table 2. Correspondence Matrix of Design Principle

Threat / Actor	Author	Publisher	Audience	Researcher	Revenger	Plagiarist
Spoofing	DP1	DP2	DP2	DP2		DP1
Tampering	DP3	DP3				
Repudiation		DP4				
Information disclosure	DP5		DP6	DP7	DP6	
Denial of service	DP8	DP8				
Elevation of privilege	DP9	DP9		DP9		

The first design principle suggests only the original author should claim for the authorship to prevent spoofing from the plagiarist. This also implies the reputation built by this publication could not be transferred, despite prior study suggests reputation transferal is socially beneficial for digital markets (Xu et al. 2018). To enforce this rule, the authorship metadata should contain indirect information of the author which could be reconstructed back to the direct information uniquely later. Conventionally, the authorship metadata like a pseudonym should be embedded with the publication together to prevent attacks like cybersquatting.

A construction that fulfills this principle is to leverage cryptographic hash function. For instance, the author of the Tether Report, a controversial article that accuses the irregularity and

unusual policies in the cryptocurrency Tether, used a 64-bytes hex string[2], which appears to be a SHA-256 hash digest, as the author's identity (1000x Group 2018). Cryptographic hash function is also commonly used in Blockchain applications such as Proof-of-Existence and Hash Time Locked Contract (HTLC). In particular, the author could construct the pseudonym token as *Token* = H(*Author* | *Secret*). The rationale to include a secret (a.k.a. salt) is to prevent revengers from pre-computing a list of hash digest of names of commonly known authors. To reveal the author's identity, one could simply broadcast the pre-image of the *Token* hash digest, i.e. *Author* and *Secret*, and anyone could easily verify. Although people other than the author could do the broadcasting, in general only the author knows the secret.

The second principle allows the author to unrestrictedly verify the identity of other users in the system, but not the other way round. As the author is the most vulnerable party in the system, this rule could prevent authors from submitting the sensitive information to the hand of malicious parties. Once the identity of the interacting party is verified, the author might start to disclose partial information on his or her identity to the recipient. Typically, this is done by using public key cryptosystem with certificate authority in the e-business context. Despite this design will depend on the robustness of the certificate authority, apparently there is no better ways to associate digital and physical identity without trusting on certain third-parties.

The third principle ensures data integrity and encourage standard format with a checksum. Unlike traditional publication systems where the author data is typically a person's name, anonymous publication systems could have very arbitrary and lengthy string as the author's identity token, which could introduce inconsistency. Using the Tether Report example, one could claim that the authorship token string could be decrypted as "Jean-Louis van der

[2] Author: 32E3690D50B3B477DF7841212D4BB938DC9CDB50307618328E7F8B53F37CC1E2

Velde@Tether"[3], which appears to be the CEO of Bitfinex. To address this issue, similar to standard communication protocols like TLS, an additional metadata regarding the encryption algorithm should be specified, and cryptographically weak algorithms should not be used.

The fourth principle aims to address the principal-agent problem for the publishers who manage an anonymous publication system. The system should have audit trails to indicate which particular individual has potential access to the author's identity, and such records should be expose to the public when an identity leakage incident happens. This is, ironically, designed for retaliation on misbehaving agents to minimize the risk of information leakage from human. However, when there are many agents had already accessed to the sensitive information, it is not trivial to investigate for the responsible parties. Hence, the principle of least privilege should be considered in the first place, and ideally eliminate the need of agency.

The fifth principle allows only the author to reveal the identity information. In practice, a common design is the author simply delegates the right of identity management to the publisher. Nonetheless, if the publisher could also be a malicious actor, the author may self-manage the identity to reduce the risk of exposure, especially with the nature of irrevocable access right. One way to control the potential malicious centralized entity is to split the access right, such that the data is accessible only when *m* out of *n* agency agree to unlock the right. This could be done by secret sharing or key splitting as in DNSSEC root key.

The sixth principle ensures the sensitive data is secure in the first place. The opt-in instead of opt-out choice also gives the author more control on the sensitive identity information. Besides the database that stores the identity information (which should be encrypted), the

[3] This ridiculous result could be obtained by applying XOR decryption on the author token "32E3690D50B3B477DF7841212D4BB938DC9CDB50307618328E7F8B53F37CC1E2", with the encryption key "788608637DFFDB02B60B61574C25995CB9EEFB06551A7C57CE2BEE279B19B3E2"

communication between the author and the publisher could also be a target for external parties to recover the identity information, which should be protected as well.

The seventh principle is to facilitate sustainable Bibliometric research without involving obscure techniques like Linguistic analysis that may misrepresent the author. This could be achieved by letting the author to disclose partial identity information that is sufficient for research without revealing the full identity. This rule should also enable researchers to assess source credibility of the publication as well. To partially reveal the source information, the author may use ring signature scheme, which could proof the author is one of the individuals in a list of entities with a public key (Rivest et al. 2001). Yet, the availability of this scheme will depend on whether the entities in the pool have published their public key. Another way is to include extra pseudonyms on the publication, which are used across different works[4]. Again, the author can control the disclosure of these extra relational identifiers.

The eighth principle suggests the need of recovery mechanism to maintain system availability. This rule actually conflicts with the fifth principle, unless the author adopted a suitable recovery mechanism beyond the system scope. A compromise between DP5 and DP8 is required to maintain proper balance between confidentiality and availability – an extreme confidential-focus system may end up with having only unrecoverable pseudonyms, whereas an extreme available-focus system could breach the privacy with only a single bad agent. For the "hide first and reveal later" designs discussed previously, a crucial dependency will be the availability of the author. For instance, the CEO of Quadriga, the biggest cryptocurrency exchange in Canada, passed away without revealing the password of the digital wallets, causing loss of $145 million worth of Bitcoin (Shane 2019).

[4] Similar to DP1 but instead of hiding a name, one can hide a random string.

To recover the information without the need of human agency, one could use a time-lock encryption, where the encrypted message could be decrypted automatically after a determined period of time. This could be done using witness encryption with a consensual public time clock such as the block height of Bitcoin Blockchain (Liu et al. 2015). For instance, suppose one wants the message to be automatically decrypted after 50 years, the required witness will be having Bitcoin block information with block height as the current height plus 2629800 (50 years divided by 10 minutes). Of course, this assumes Bitcoin still exists after 50 years.

However, most of the witness encryption schemes are not practically implemented. Theoretically, the scheme may even define certain arbitrary condition like "automatically decrypt when Enron goes bankrupt" for whistleblower in Enron. Another more practical way for time-lock encryption is to use proof-of-work like in Bitcoin mining. The difficulty level could be set such that it requires brute-forcing for certain period of time on average. Yet, it requires extra uncompensated computation power exert by some parties.

Last but not least, the ninth principle suggests a granular access control mechanism to prevent elevation of privilege. A typical tactic to ensure data privacy is through pooling individuals into groups, such as specimen pooling in epidemiologic studies (Saha-Chaudhuri and Weinberg 2017). To implement this, the system may allocate a shared identifier to every individuals in the same category. But this will also allocate the same access right to the users in this group, which is undesirable with the presence of multiple independent actors in the system.

DISCUSSION

This study presents nine design principles for an anonymous publication system to address the trilemma for authors regarding privacy, attribution and dependency. The PETs discussed in this study, including cryptographic hash function, public key cryptosystem, ring

signature and time-lock encryption could be combined to fulfill the design principles. Platform developers could integrate these technologies to build a Blockchain-based decentralized system to facilitate anonymous publication. Despite the purposed system could be less depend on human, the current infrastructure may not be ready to fully realize the value of such a system. In particular, ring signature scheme is less valuable without a large pool of public key linked with physical identity, and time-lock encryption is infeasible without the proper implementation. In addition, the design principles proposed in this study are mainly based on threats to the first party (i.e. the author). Further research should be conducted to address other threats on the system, such as a threat actor publishes on behalf on other people.

REFERENCES

1000x Group. 2018. "Quantifying the Effect of Tether."

Abbasi, A., and Chen, H. 2005. "Applying Authorship Analysis to Extremist-Group Web Forum Messages," *IEEE Intelligent Systems, 20*(5), pp. 67-75.

Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research, 17*(1), pp. 61-80.

Dixon, O. 2016. "Honesty without Fear - Whistleblower Anti-Retaliation Protections in Corporate Codes of Conduct," *Melbourne University Law Review, 40*, pp. 168-206.

Ferguson, C., Marcus, A., and Oransky, I. 2014. "Publishing: The peer-review scam," *Nature News, 515*(7528), pp. 480.

Fitzgibbon, W. 2018. "Defamation case could be a 'killer' for Namibia's largest daily paper." (https://www.icij.org/blog/2018/09/defamation-case-could-be-a-killer-for-namibias-largest-daily-paper/, accessed October 13, 2019).

Hanel, P. H. 2015. "Why scientific publications should be anonymous," *arXiv preprint arXiv:1512.05382*.

Holmes, D. I. 1994. "Authorship attribution," *Computers and the Humanities, 28*(2), 87-106.

Howard, M., and LeBlanc, D. 2003. "Writing secure code."

Hui, K.-L., Tan, B. C., and Goh, C.-Y. (2006). "Online information disclosure: Motivators and measurements," *ACM Transactions on Internet Technology (TOIT), 6*(4), pp. 415-441.

Kharif, O. 2019. "John McAfee Vows to Unmask Crypto's Satoshi Nakamoto, Then Backs Off." (https://www.bloomberg.com/news/articles/2019-04-23/john-mcafee-vows-to-unmask-crypto-s-satoshi-nakamoto-within-days, accessed October 13, 2019).

Lazer, D., Baum, M., Benkler, Y., Berinsky, A., Greenhill, K., Menczer, F., ... Schudson, M. 2018. "The science of fake news," *Science, 359*(6380), pp. 1094-1096.

Liu, J., Garcia, F., and Ryan, M. 2015. "Time-release protocol from bitcoin and witness encryption for sat," *IACR Cryptology ePrint Archive*, pp. 482.

Lowry, P. B., Moody, G. D., Galletta, D. F., and Vance, A. 2013. "The drivers in the use of online whistle-blowing reporting systems," *Journal of Management Information Systems, 30*(1), pp. 153-190.

Madore, P. H. 2019. "Crypto Twitter Calls Craig Wright Out on Satoshi Claim, Again." (https://www.ccn.com/crypto/crypto-twitter-calls-craig-wright-out-on-satoshi-claim-again/2019/06/14/, accessed October 13, 2019).

Mazzone, J. 2006. "Copyfraud," *New York University Law Review, 81*(3), pp. 1026-1100.

Merton, R. K. 1968. "The Matthew effect in science: The reward and communication systems of science are considered." *Science, 159*(3810), pp. 56-63.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."

Neuroskeptic. 2013. "Anonymity in science," *Trends in Cognitive Sciences, 17*(5), pp. 195-196.

Rains, S. A. 2007. "The impact of anonymity on perceptions of source credibility and influence in computer-mediated group communication: A test of two competing hypotheses," *Communication research, 34*(1), pp. 100-125.

Rieh, S. Y. 2010. "Credibility and cognitive authority of information," *Encyclopedia of Library and Information Sciences,* pp. 1337-1344

Rivest, R. L., Shamir, A., and Tauman, Y. 2001. "How to leak a secret," *International Conference on the Theory and Application of Cryptology and Information Security*

Rossiter, M. W. 1993. "The Matthew Matilda effect in science," *Social studies of science, 23*(2), pp. 325-341.

Saha-Chaudhuri, P., and Weinberg, C. R. 2017. "Addressing data privacy in matched studies via virtual pooling," *BMC Medical Research Methodology, 17*, pp. 136.

Shane, D. 2019. "A crypto exchange may have lost $145 million after its CEO suddenly died." (https://edition.cnn.com/2019/02/05/tech/quadriga-gerald-cotten-cryptocurrency/index.html, accessed October 13, 2019).

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information privacy research: an interdisciplinary review," *MIS Quarterly*, pp. 989-1016.

Southurst, J. 2014. "*Hacker Hijacks Satoshi Nakamoto's Email, Threatens to Reveal All*." (https://www.coindesk.com/hacker-hijacks-satoshi-nakamoto-email, accessed October 13, 2019).

Stamatatos, E. 2008. "A survey of modern authorship attribution methods." *Journal of the American Society for Information Science and Technology, 60*(3), pp. 538-556.

Student. 1908. "The Probable Error of a Mean," *Biometrika, 6*(1), pp. 1-25.

Sum, L.-k. 2018 "Public interest defence could spare newspaper from legal troubles in TransUnion credit exposé, lawyers say," (https://www.scmp.com/news/hong-kong/law-and-crime/article/2175694/public-interest-defence-could-spare-newspaper-legal, accessed October 13, 2019).

Wainberg, J., and Perreault, S. 2015. "Whistleblowing in audit firms: Do explicit protections from retaliation activate implicit threats of reprisal?" *Behavioral Research in Accounting, 28*(1), pp. 83-93.

Whittaker, Z. 2018. "*Lawsuits threaten infosec research — just when we need it most*." (https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/, accessed October 13, 2019).

Xu, H., Chen, J., and Whinston, A. B. 2018. "Identity management and tradable reputation," *MIS Quarterly, 42*(2), pp. 577-593.