Using Payment Gateways to Maintain Privacy in Secure Electronic Transactions

Alapan Arnab and Andrew Hutchison

Data Network Architectures Group
Department of Computer Science
University of Cape Town
{aarnab, hutch}@cs.uct.ac.za

Abstract. Because many current payment systems are poorly implemented, or of incompetence, private data of consumers such as payment details, addresses and their purchase history can be compromised. Furthermore, current payment systems do not offer any non-repudiable verification to a completed transaction, which poses risks to all the parties of the transaction – the consumer, the merchant and the financial institution. One solution to this problem was SET, but it was never really a success because of its complexity and poor reception from consumers. In this paper, we introduce a third party payment system that aims to preserve privacy by severing the link between their purchase and payment records, while providing a traceable transaction that maintains its integrity and is non-repudiable. Our system also removes much of the responsibilities placed on the merchant with regards to securing sensitive data related to customer payment, thus increasing the potential of small businesses to take part in e-commerce without significant investments in computer security.

1 Introduction

In February 1996, the two leading credit card companies, Mastercard and Visa, together with a number of other companies like IBM started a process to create standardised payment processes and the security thereof [9]. Their result, Secure Electronic Transaction (SET) specification, was more than a security protocol for electronic payments, and encompassed the entire business transaction process. While technically lauded [3, 8] SET has never been a success [7, 6], for a number of reasons, including the complexity in implementation, cost of implementation and reluctance from customers.

Some of the security features offered by properly implemented SET system include:

1. end to end secure communication amongst all parties involved in the payment transaction
2. establishment of trust for all parties in a transaction
3. privacy of the consumer's payment details from the merchant
4. privacy of merchant's sale details details from the payment gateway

With the absence of SET, e-commerce sites have implemented their own payment systems, and except for the spread of the use third party certified digital certificates by merchants and the use of encrypted communication channel (usually through the use of SSL or TLS) between the consumer and the merchant, nothing in the payment process can be considered standardised. This creates a great risk for consumers as their data can be compromised by the merchant due to inadequate protection or incompetence [3] or collected for sending spam to the consumer [5].

Another problem with current systems is that the consumer has to trust that the merchant will carry out the transaction correctly, and that there is adequate security in the communication links between the merchant and the bank. Furthermore, receipts produced by the merchant cannot be verified to confirm that the amount reflected on the receipt is the same as the amount actually charged. If a dispute were to arise, the consumer has to prove that the merchant's transaction service is at fault as opposed to an attempted fraud by the consumer. Thus, the status quo presents great privacy and security risk to the consumer.

In this paper, we re-examine the use of a third party payment service. A payment gateway, ideally operated by a trusted financial service for secure electronic transactions, with a main aim to promote the privacy of the parties involved.

2 Requirements

There are a number of requirements for electronic transactions, and we have identified the following key requirements, which we drafted from a number of different systems including SET and other research in this area [5, 10, 2].

2.1 Secure communication between all parties

There needs to be secure communication channels between all parties involved in a transaction. It is necessary to ensure that information is not revealed to parties not involved in the transaction regardless of the importance of the information, and that the integrity of the communication is preserved.

2.2 Minimise the sharing of data between the parties

There are two different aspects to this requirement:

1. The payment service (referred to as the payment gateway) does not need to know the details of the subject of the transaction. This is particularly important if the subject of the transaction is of sensitive nature, especially if the subject is not held in high regard in the consumer's community.
2. The merchant does not need to know the payment details of the subject other than the confirmation that the payment has succeeded. In many cases, the consumer may not want to build a relationship with the merchant, because the purchases are in-frequent (holiday travel for example). Thus, it is in the consumer's best interest

to reduce the amount of information shared with the merchant. There are also cases where the purchaser is not the end consumer of the service or product, for example in the case of gift purchases such as flowers. In such a case, it is not reasonable to collect purchaser details when they have very little in connection to the consumer.

2.3 Support a number of payment mechanisms

The credit card is the dominant payment tool on the Internet, but it is not necessarily available to everyone [5, 7]. Integrating other payment mechanisms such as debit cards, bank transfers, cheques or even other payment services such as PayPal is costly for the merchant, but a payment gateway can handle multiple payment services if there are a sufficient number of consumers spread over a number of different merchants that would be willing to use it.

2.4 Traceability and verification of transactions

In [10], the authors discuss how traceability of transactions is an important requirement in building trust. Traceability of a transaction allows for the correct auditing, provides for accountability with the implementation of associated security policies as well as a mechanism for verification of the transaction [10]. As discussed earlier, current transaction receipts offered by e-commerce sites provide neither non-repudiation nor integrity, and are thus not suitable for traceability or verification.

2.5 Merchant Authentication

It is necessary to link merchants to the payments from consumers, and there is a need to confirm that the merchant is accepted by the payment gateway. This promotes a secondary layer of trust for the consumer in that the merchant is an entity that is still operating and in business.

2.6 Minimal set up cost and infrastructure

Ideally, electronic transactions should not require large investments from any of the parties involved. One of the problems with the full implementation of SET was the requirement that every customer needed a digital certificate. This represented a sizable investment from the customer as well as third parties who needed to issue, verify and maintain these digital certificates.

3 The Payment Gateway

3.1 System Operation

Our system differs from the traditional payment mechanism by separating the sale of products and services of the merchant, and the payment transaction between the

consumer and the payment gateway. The payment gateway is intended to be a financial web service, catering for a number of different merchants, but, at the same time not resembling a bank. In many cases, consumers do not need or want a relationship with the merchant or the payment system beyond their immediate transaction. Thus, the process of registering users and allowing transfers of money between registered users (like Paypal) is not the aim.

One of the main functions of a bank is to provide their clients with suitable means to conduct commercial transactions like providing a checking service or issuing credit cards. For this reason, Paypal can be seen as a bank, as they provide the means for their clients to conduct electronic transactions. In contrast, the payment gateway we present in this paper acts as an agent who helps in concluding financial transactions between the merchant and the client.

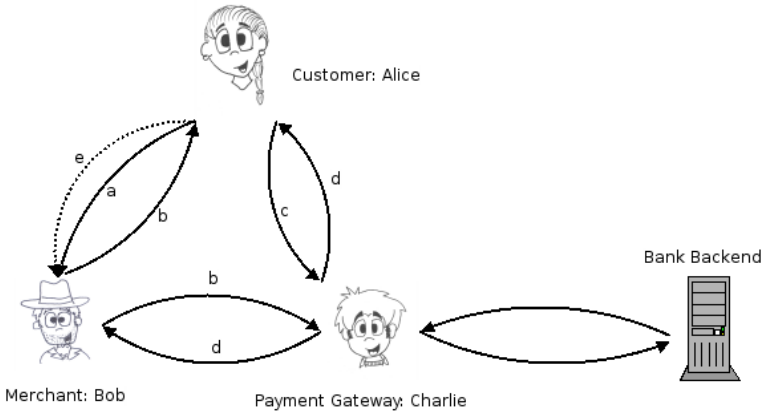

Fig. 1. Overview of the Payment Gateway System

Figure 1, gives an overview of our proposed system, comprising of four players: a bank (or similar financial institution), the payment gateway, the merchant and the consumer. The payment gateway has a secure connection to the bank which provides verification of credit cards and carry out the actual financial transaction.

After the consumer has finished shopping (step a in figure 1), the merchant creates a signed invoice for its services and products for the consumer. Another invoice with four components – a globally unique verifiable identifier (all documents will have verifiable globally unique identifiers through the use of schemes such as the one described in [1]), the amount payable (and its terms e.g. payment in full or in installments), a globally unique merchant identifier (issued by the payment gateway) and a digital signature of the invoice – is created for the payment gateway. These invoices are forwarded to the respective parties (step b). The second invoice has no details concerning the consumer, and thus the details of the sale is completely masked. The digital signature assures non-repudiation on the value of the sale and performs authentication on behalf of the merchant. Furthermore, this approach allows for non-real time communication

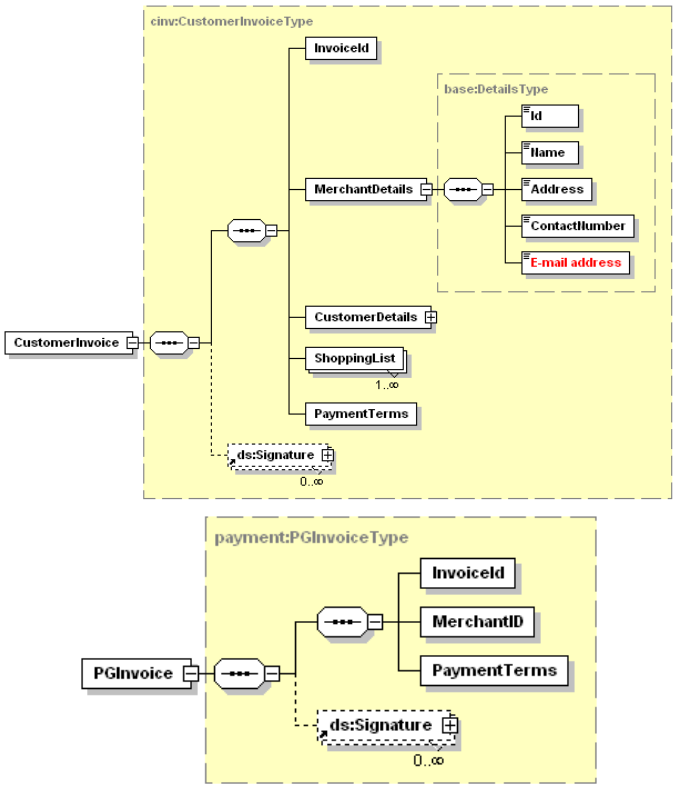

Fig. 2. XML schema diagrams for a customer invoice (left) and one for the payment gateway (right)

between the merchant and the payment gateway. XML schemas describing how such invoices could look are shown in figure 2.

The consumer is also not required to pay immediately (although the merchant is not required to perform its duties without being paid), and can shop at other merchants if they want to. The consumer can thus pay many invoices to the payment gateway within one transaction (step c), and it is the payment gateway's responsibility to allocate the receipts accordingly. Once the payment is processed, the payment gateway creates two receipts (step d). For the consumer, the payment gateway lists the terms of payment (e.g. credit card, bank transfer etc.), the identifiers of the invoices being settled and an unique identifier which is then digitally signed. For the merchants, the payment gateway creates a signed receipt listing the merchant identifier, the invoice identifier, the identifier of the consumer's receipt, an unique identifier for the merchant's invoice and the amount. Depending on the set up, this receipt could contain a number of invoices collected on the merchant's behalf since the last receipt. XML schemas describing how such receipts could look are shown in figure 3.

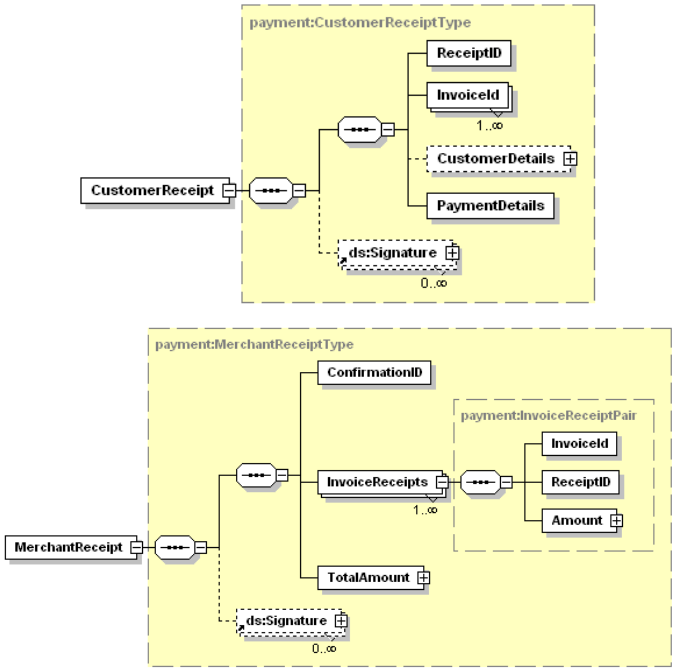

Fig. 3. XML schema diagrams for a customer receipt (left) and one for the merchant (right)

Like the invoices generated by the merchant, digital signature assures non-repudiation and authenticates the payment gateway. The merchant also does not learn any details on how the consumer paid for the goods, and in fact cannot even ascertain whether the recipient of the goods and services and the purchaser are the same. Thus the privacy of the consumer is secured. In step e, the consumer can use his/her receipt to prove that the services were paid for in the case of a dispute.

3.2 Security Considerations

Chain of Trust To provide trusted digital certificates, trusted third party certified digital certificates are required. However, unlike the full implementation of SET [3, 9], users do not require digital certificates to take full advantage of the benefits.

Secure Communication The communication between the bank backend and the payment gateway must be secure. However, it is easier to guarantee and audit one such service as opposed to every merchant wishing to perform secure transactions. SSL/TLS can be used to secure communication between the consumer and the payment gateway, and thus the consumer does not require his/her own digital certificate, although mutual authentication would be preferred. Communication between the payment gateway and the merchant can either be secured through an encrypted tunnel such as SSL/TLS or

through the use of XML encryption. The later is possible as both parties have each other's public keys (to verify digital signatures).

Authentication There is no authentication of the consumer, and thus it could be possible for the consumer to be totally anonymous during a payment transaction. Merchants are authenticated using their digital signature. The merchant identifier serves as an additional layer of authentication, but is aimed more for easier administration.

Minimise Data Sharing The only data shared between the payment gateway and the merchant are identifiers to link transactions and the payment amount. Like SET's dual signature scheme, payment details and merchant's sale details remain hidden from the non-participating parties. Furthermore, unlike SET where it is not possible to prove that the payment gateway is known by the consumer [3], it is possible to show that the customer is aware of all the parties involved in the transaction, and can potentially even have a choice in the payment gateway.

Traceability and Verification The use of digital signatures allow for the verification of each step of the payment transaction. It is possible to trace the entire payment process, should it be required (during a criminal investigation for example), if both the merchant's and the payment gateway's records are matched. An examination of one party's records is not going to be enough to reveal the complete picture, thus achieving the privacy goals, without compromising traceability.

4 Potential uses of payment gateways

4.1 DRM and online services

In [4], the authors discuss how consumers expect almost no relationship between the rights holders of content and themselves, once they purchase a copy of the content. They argue that DRM breaks that mould, with the potential for the rights holder to monitor both the purchase and the use of the content. The payment gateway service was initially developed as a mechanism to break one part of such a relationship, and forms part of a wider DRM project. In the case of DRM, it is also necessary to cater for scenarios where the payment is at a future date (for example: consumer can use product until a certain date, and is then required to pay for additional usage). No current DRM system can accommodate such a scenario as they do not have any payment verification support. Since our receipts are machine readable, and verifiable, it is easy to incorporate such a mechanism.

There are also other online services for which the consumer would either like privacy due to their sensitive nature (adult entertainment for example) or would not like to establish long relationships because of their short nature (once off donations or Wi-Fi hotspot purchases while travelling for example).

4.2 Small Business

The Internet presents great opportunities for small businesses for wider market access. However, setting up and running a secure e-commerce site is a costly exercise. Because of this, less established businesses have a lower degree of trust from consumers when compared to their more well established rivals. A payment gateway system as described here has the potential to increase the trust that is placed in such a business due to two factors:

1. It is easier to conduct regular audits and ensure the security of a few payment gateways instead of auditing and securing every online payment system. Payment gateways can also publicise these audits in order to establish a higher degree of trust in the payment gateway.
2. Businesses which have a relationship with established payment gateways are less likely to be phishing scams or conduct other fraudulent activities, as there is a higher chance of being monitored.

For these reasons, payment gateways could be of great use for smaller, less established online e-ventures.

4.3 Digital Vouchers

Instead of the merchant initiating the transaction, it could be possible for the customer to pay upfront, in return for a redeemable voucher. This voucher can then be presented to the merchant as payment for services/product. To avoid duplication of vouchers, redemption of vouchers need to be real time atomic transactions; but the infrastructure described in this paper does not need to be significantly changed to accommodate vouchers.

We think that one of the main uses of vouchers could be in the realm of micro payments. The customer could buy low denomination vouchers (for example one hundred 10 cent vouchers) and then exchange these vouchers for products or services. The redeemed vouchers can be paid out in bulk at the end of the day (or even week or month), thus reducing the costs of the transaction.

5 Economics and Practicalities of running a payment gateway

In section 4, we discussed at least two areas where we think a payment gateway will be more effective that current payment systems. In this section, we briefly examine the potential business case/practicalities offered by our proposed system, as well as a few related issues.

5.1 Running a third party payment service

The main aim of a payment gateway is to serve as a payment point for a number of different merchants, and thus the payment gateway will have to charge the merchants

for such a service. Thus, this service will only make sense for any merchant if this solution is cheaper when compared to implementing the payment service on their own.

There is effectively two sets of costs for any payment service, whether implemented by the gateway or the merchant: the cost of implementation and maintenance of a secure processing service and the transaction costs of processing payments.

Implementation and Maintenance Costs In either approach, a base security implementation cost is incurred, as the merchant will still be required to implement security to protect customer data. There will also be an initial set up cost to integrate the receipt/invoice system to the merchant's billing system. In either approach, we estimate that there will be no significant difference in costs, if the merchant only adopts one payment mechanism. If the merchant implements other payment mechanisms, additional costs are incurred, which are not comparable in the case of using a payment gateway.

However, one cost that is not often taken into account is the legal and regulatory costs associated with collecting data from customers. As discussed in [11], an increase in data collection from consumers increases the privacy risk ceiling for a collector, which has a significant increase in security costs. Thus, collecting and processing payment details from consumers will have an increase in costs, when compared to simply collecting data to provide the associated service, especially if the service is delivered on the Internet, thus not usually requiring the customer's private details.

Transaction Processing Costs Transaction processing costs stem from charges levied by credit card and other financial companies for completing the transaction. These charges form a significant cost for the merchant, and can be as high as 5% of the value of the transaction.

Business Case for the use of a Payment Gateway The payment gateway could take advantage of a higher volume of transactions, as they will process more transactions than a single merchant. Consequently, payment gateways can be in a position to negotiate better transaction processing charges than individual merchants. Thus, it should be possible for the payment gateway can charge the merchant lower than the financial institution, but still maintain a significant margin on their own costs.

Another value of the payment gateway is the potential to cater for different payment types. Again, with a higher volume of transactions; a higher number of merchants can cater for different payment types; without significant investment in such payment mechanisms.

Core to the success of a payment gateway will depend on the trustworthiness of the system; and thus they will need to have verifiable, well known, security audits that can be used to build customer trust. This can also be used as a marketing strategy to convince merchants to join the system.

It will still be possible to create relationships between the consumer and the merchant, through the use of customer logins etc. However, this will no longer be a requirement as it is currently for many e-commerce systems. Thus, it would be possible for merchants to device incentives for customers to maintain a long lasting relationship, but without loosing sales from consumers who do not wish to make such relationships.

5.2 Returns and Charge Backs

A direct problem with anonymous payments arises in the scenario when a product is returned or the merchant returns part (or the full) of the payment back to the customer. While receipts issued by the payment gateway can be used by the customer to prove their original payment, charge backs are not possible. One potential solution to this problem, would be the use of vouchers as explained in section 4.3. If the customer is also signed up as a merchant, then they can redeem the voucher directly. Alternate voucher redemption plans into other monetary units could also be considered.

6 Comparison to Similar Services

There are a number of payment systems used on the Internet, and in this section, we compare our system to some of these systems. Many of these systems are proprietary, and few published details are available on how their backend works.

6.1 RegNet (http://www.regnet.com)

RegNet (and other similar websites) offer secure payment solutions for digital software licenses. They offer a huge catalogue of products from a number of different vendors, and they are in effect an shopping site for software licenses, although, like our payment gateway, they do not handle the subject of the transaction. However, unlike our payment gateway, they have complete detail on what the customer purchases, and in the case of most licenses, how long the licenses are and for what purposes the licenses are being purchased.

6.2 PayPal (http://www.paypal.com/)

PayPal is one of the most established payment systems around, originating as a mechanism to pay for auction purchases on e-Bay. Like our payment gateway, PayPal also ensures dual privacy – the merchant does not know the payment details of the consumer, and PayPal does not know the sale details of the merchant.

However, PayPal is more than a payment mechanism; and can be more appropriately described as a bank. In PayPal, both the consumer and the merchant have to be registered, and with some exceptions, both parties can receive and pay money to other PayPal account holders. Because of this restriction, PayPal cannot operate in every country.

Another difference between our system and PayPal is the provision of signed receipts and invoices; although these can probably be easily added to PayPal.

6.3 Google Checkout (http://checkout.google.com/)

Google Checkout is one of the newest payment systems, released in mid 2006, and in many respects, it is similar to RegNet as opposed to PayPal and our payment gateway.

Like RegNet, Google Checkout offers a secure payment solution for multiple online stores, preserving customer payment privacy. However, unlike PayPal and our payment gateway, Google Checkout has a complete detail on what was purchased by the consumer. Thus, like RegNet, it is an electronic store that does not handle the subject of the purchase.

7 Conclusion

In current e-commerce systems for the Internet, the customer has to place a high degree of trust in the merchant, that the merchant will process the transaction correctly and handle the details of the transaction in a secure manner. Furthermore, merchants force the customers to create relationships, collecting data that is sometimes unnecessary, increasing the risks for the customer when computer security breaches occur.

In this paper, we have presented a payment gateway system that preserves privacy for all the parties involved in the transaction, as well as minimises the risks to data security for consumers. Furthermore, the system also provides traceability of all transactions, complete with signed invoices and receipts for both merchants and customers that provide integrity and non-repudiation; properties that are not possible in most of the current payment systems. The invoices and receipts are machine readable and thus can be used as payment tokens or proof of payment for various services, including DRM systems and web based services.

8 Acknowledgements

XML schema diagrams generated using XML Spy 2004.

This work is partially supported through grants from the University of Cape Town (UCT) Council and the National Research Foundation (NRF) of South Africa. Any opinions, findings, and conclusions or recommendations expressed in this paper/report are those of the author(s) and do not necessarily reflect the views of UCT, the NRF or the trustees of the UCT Council.

References

1. ARNAB, A., AND HUTCHISON, A. Verifiable digital object identity system. In *Proceedings of the Sixth ACM Workshop on Digital Rights Management, Co-Located with ACM CCS 2006, Alexandria, Virginia, USA* (2006), K. Kurosawa, R. Safavi-Naini, and M. Yung, Eds., ACM.
2. BASU, A., AND MUYLLE, S. Authentication in e-commerce. *Communications of the ACM 46*, 12 (2003), 159–166.
   url: http://doi.acm.org/10.1145/953460.953496.
3. BELLA, G., PAULSON, L. C., AND MASSACCI, F. The verification of an industrial payment protocol: the set purchase phase. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security* (New York, NY, USA, 2002), ACM Press,

pp. 12–20.
url: http://doi.acm.org/10.1145/586110.586113.

4. MULLIGAN, D., HAN, J., AND BURSTEIN, A. How DRM Based Content Delivery Systems Disrupt Expectations of "Personal Use". In *Proceedings of the 2003 ACM workshop on Digital Rights Management* (2003), ACM, pp. 77–89.
URL: http://doi.acm.org/10.1145/947380.947391.
5. PEHA, J. M., AND KHAMITOV, I. M. Paycash: a secure efficient internet payment system. In *ICEC '03: Proceedings of the 5th international conference on Electronic commerce* (New York, NY, USA, 2003), ACM Press, pp. 125–130.
url: http://doi.acm.org/10.1145/948005.948022.
6. ROBERTS, P. Strong authentication a hard sell for banks. *ComputerWorld* (02 Nov 2004).
URL: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=97133
Last accessed: 05 Aug 2006.
7. ROSENCRANCE, L. Gartner survey sparks debate on internet retail fraud. *ComputerWorld* (18 July 2000).
URL: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=47270
Last accessed: 05 Aug 2006.
8. RUIZ, M. C., CAZORLA, D., CUARTERO, F., AND PARDO, J. J. Analysis of the set e-commerce protocol using a true concurrency process algebra. In *SAC '06: Proceedings of the 2006 ACM symposium on Applied computing* (New York, NY, USA, 2006), ACM Press, pp. 879–886.
url: http://doi.acm.org/10.1145/1141277.1141480.
9. STALLINGS, W. *Network Security Essentials – Applications and Standards*, international second ed. Prentice Hall, 2003.
10. STEINAUER, D. D., WAKID, S. A., AND RASBERRY, S. Trust and traceability in electronic commerce. *StandardView 5*, 3 (1997), 118–124.
url: http://doi.acm.org/10.1145/266231.266239.
11. TSAI, J. Y., CRANOR, L. F., AND CRAVER, S. Vicarious infringement creates a privacy ceiling. In *Proceedings of the Sixth ACM Workshop on Digital Rights Management, Co-Located with ACM CCS 2006, Alexandria, Virginia, USA* (2006), K. Kurosawa, R. Safavi-Naini, and M. Yung, Eds., ACM.