

Security and Lock-In

Tom Lookabaugh and Douglas C. Sicker

Department of Computer Science and
Interdisciplinary Telecommunications Program
University of Colorado at Boulder

[Tom.Lookabaugh,Douglas.Sicker]@colorado.edu

Work in Progress

Presented at Economics and Information Security Workshop
University of Maryland
May 29-30, 2003

Introduction

A customer experiences “lock-in” when switching costs exceed the potential incremental value of alternative suppliers’ products over its current supplier’s product. Customers may regret this state of affairs if they would have been better off having secured the alternative product from the start, or more simply, if the switching costs were substantially lower than the incremental value of the alternative supplier’s product (in which case, they would switch and capture the difference). Conversely, an incumbent supplier might appreciate and indeed encourage this state of affairs to the extent it can realize additional profit. These two interact in the sense that a supplier would likely forego additional profit (and a customer would receive lower prices) if switching costs were lower, even if the customer does not actually switch. Less apparently, though potentially more importantly, lock-in may have substantial impact on the types of product innovation a customer accesses, both directly from its supplier and indirectly through innovation in complementary products.

Computer and communication security (hereafter simply security) seems particularly suited as a locus of lock-in by virtue of several factors: (i) it can be manifested as a technical compatibility requirement that must be met by a variety of applications and pieces of equipment communicating locally or across a network, (ii) suppliers may explicitly or implicitly suggest that proprietary security is better than open security since the supplier can control access to information about the system, (iii) it may be difficult to segregate permissible competitive reverse engineering from illegitimate piracy.

The *possibility* of security induced lock-in is not, by itself, that interesting. It becomes interesting if it actually occurs, it has non-trivial consequences, and there exists at least one other feasible state of affairs that would be preferable to some party. All three of these are important points that require both a theoretical framework and empirical evidence. They are challenging to tackle as they span technical, economic, business, and legal domains. Once established, though, they have implications for many parties, including customers, suppliers, and policy makers.

In fact, a number of candidate examples of security based lock-in exist, including conditional access systems (also known as rights management systems) used in the cable industry, cartridge compatibility (video games, printers), security in wireless LAN protocols, hardware and software security for the PC, private key cryptography in various applications, and a number of others.

Theoretical Framework

The Role of Security in Lock-In

Many security systems include protocols that describe how messages are to be transmitted securely or how various components of a system (local or distributed) are to interact to perform a secure action. Conformance to such protocols creates a compatibility requirement across system components. A supplier that wishes to sell a system component will either need to be compatible with the necessary security protocols, or must provide sufficient additional value to motivate a customer to replace all other system components that require those security protocols. In this latter case, the cost of replacing other system components becomes a switching cost and a source of lock-in. If the installed base that must be replaced is large, the cost can be prohibitive.

New suppliers attempting to circumvent security based lock-in without requiring wholesale replacement of compatible components will typically look to implement the necessary existing protocols. They may attempt to do so without the permission of those that originated, own, or otherwise control the required protocols. This may be technically feasible (e.g., if the information is public or by reverse engineering if it is not), but can be stymied by intellectual property law: the necessary information may be protected by various copyright and patent rights. This is, in fact, also true for the general case of technical compatibility based lock-in, but the effect is sharpened in the case of security because of the potential difficulty in distinguishing what might be considered legally protected reverse engineering activities for competition reasons from attempts to foster piracy for reasons of illegitimate access to messages or content. This particular effect has been manifested recently in controversy around application of the Digital Millennium Copyright Act. Originally created to outlaw circumvention by pirates of technology to protect intellectual property, the act is seeing broader application in preventing reverse engineering, such as a recent case in which an injunction was secured by Lexmark against a developer of chips that enable “clone” printer cartridges [11].

Alternatively, a new supplier may seek to license the necessary security protocols from the owner. If the owner is the incumbent supplier, this should be feasible providing the incumbent supplier can extract the profit it forgoes for each product not sold from the new supplier through a license fee or equivalent compensation. But, it may be difficult to achieve this solution. If, for example, the new supplier’s advantage is more efficient manufacturing and it can offer the product to the customer for a lower price than the incumbent, the manufacturing efficiency cost improvement must exceed the sum of the incumbent supplier’s required unit profit *plus* the new supplier’s required unit profit. Anything short of this will not present a solution as the licensed new supplier’s product would, in fact, be more expensive than the original incumbent’s product and hence not salable (rendering a licensing agreement moot). A second problem is that the incumbent supplier may correctly calculate the cost of profit foregone as larger than the

apparent difference between product price and product cost by taking into account other costs such as reduced economies of scale and learning, effects on cross-subsidization among the suppliers products (for example, in the printer industry, low printer margins are offset by high cartridge margins), reduced marketing and sales effects that are driven by market share, and increased costs in terms of supporting licensees (for example, restricted ability to unilaterally make system changes that involve security protocols). Importantly, even if a licensing arrangement is feasible, the full cost of lock-in is still borne, now by the customer and the new supplier jointly, and accrues as profit to the incumbent supplier.

Security also has the potential to play an enhanced role in lock-in by virtue of the perceived value of system secrecy. Suppliers may explicitly or more discretely claim that their proprietary system is more secure than, say, a potential or actually openly available alternative, since the supplier can control access to information about the system itself. This has the virtue of appealing to a common sense proposition that for a system of a given security level, reduced knowledge about the system will not help and could reasonably be expected to hinder an attacker (at a minimum, by increasing the cost of attack by the amount required to learn about the system). Notwithstanding the potential effectiveness of this position in sales calls, it is one of the most controversial points of philosophy in security system design, designated (primarily by its critics) as “security by obscurity.”

The case against security by obscurity derives from original design principles of Auguste Kerchoffs, a 19th century French military cryptographer who maintained that good security system design means relying only on the secrecy of the key and not of the security mechanism itself [7]. From the military cryptography perspective, this reasonably accounts for the likelihood that security devices will eventually fall into enemy hands (either by capture or treason). Interestingly, this case still arises in the case of current commercial information technology security, as witnessed by a recent example in which a temporary worker at a document processing firm published the details of DirecTV’s security system on the web after seeing them while his firm was employed assisting a legal firm in DirecTV’s litigation with its security supplier [1]. But, more recent arguments against security by obscurity tend to rest on two related points: (1) security inventors who rely on secrecy tend to over rely on it, making mistakes in security implementation that are later discovered by attackers, often resulting in catastrophic security failure and (2) there is a large community of peer experts who are willing to review security protocols if made public and who are likely to uncover critical flaws prior to use of a system (and perhaps even recommend appropriate fixes) [15].

The arguments for and against the beneficial role of system secrecy in security do not appear to be resolvable in any universal fashion. The debate has been sharpened recently by discussions of the relative security of open source and closed source software development. While many treatments take a position of orthodoxy (almost every one cites Kerchoffs) or speak to the experience of the community, treatments that attempt to delve deeper into whether obscurity never helps or whether open peer review is always superior (or even usually superior) tend to come up ambivalent [3, 9, 10, 14]. The lack of a simple and compelling argument that “proves” Kerchoffs means that we can expect “security by obscurity” to continue to play a role in security induced lock-in.

Implications of Lock-In

The economic theory of lock-in has been playing an increasing role in economic, business, and policy thought, particularly since the 1980's. The key impetus for this interest comes from explicit consideration of increasing returns to scale, in which each increment of economic activity is increased in value by the amount that has already occurred, resulting in the potential of positive feedback. Much traditional economics relies on diminishing marginal returns to scale, resulting in negative feedback, and reasonably associated with limited resources; as production increases, the price of inputs ultimately is bid up, resulting inevitably in declining marginal returns. But two phenomena particularly important in the information age have the potential to show unbounded increasing returns: information or knowledge itself and network effects in which the value of access to a product increases with the number of other users of that product.

Modeling of economic processes with positive feedback deviates from traditional analysis of declining marginal returns; in particular, the usual and powerful proofs that market based systems converge to unique and globally optimal equilibria no longer apply. It is conceivable, in the presence of positive feedback, that more than one stable equilibrium may exist, and that an economic system will tend to get locked-in to only one of them, not necessarily the globally optimal one [4].

While the theoretical possibility of such lock-in is not contested, the empirical evidence and the practical importance of lock-in is. Liebowitz and Margolis, for example, question first whether popular examples of lock-in actually demonstrate a non-trivial penalty between the locked-in state and a feasible alternative state, and secondly whether the effect is in fact important if there is a tendency for switching costs to ultimately be overcome regardless, typically by technological upheaval, leading to a more benign process of serial lock-in [8]. Their critique is a strong argument for the necessity of careful collection and analysis of data to support the potential theoretical consequences of lock-in.

Beyond the need for empirical evidence of lock-in and its significant and detrimental effects, we also need to consider the possibility that customers and suppliers correctly anticipate the effect of lock-in and negotiate offsetting compensation [16]. This seems particularly feasible when customers are concentrated and so can more easily internalize the effects of decisions across the customer set (importantly, internalizing network externalities). A customer and a supplier, anticipating the cost of lock-in before it has occurred might simply negotiate a compensating up front discount that is sufficient to compensate for the lock-in. Of course, they may be wrong (in either direction) as to the cost of lock-in, but this is equivalent to the normal uncertainty in negotiating current contracts intended to cover future eventualities.

An effect that may be substantially more difficult to correctly anticipate, though, and one that has been less examined in the literature in spite of its importance to the premise of serial lock-in (but see [12]), is the impact of lock-in on access to innovation. A locked-in customer will not access the potential benefit of an innovation that is not compatible with its supplier's product unless that benefit exceeds the necessary switching costs. This occurs whether the innovation is a direct product innovation or one that arises in complementary products. Trends in understanding of innovation are relevant here,

having vacillated between the neo-Schumpeterian thesis that innovation will necessarily concentrate in the largest firms to recent fascination with the innovative capability of technology start-ups, and settling seemingly into a notion that important types of innovation occur in companies of all scales [6, 13]. The relevant point, here, is that although a locked-in customer can reasonably expect some important types of innovation to be executed by its supplier, there is also a high likelihood that other potentially interesting innovations will not, so that the cost of denied access to innovation via lock-in could be substantial up to the point that such costs exceed the switching costs. Even harder to gauge but, again, potentially quite significant, is the possibility that useful innovations will never be pursued at all because of the perceived low likelihood of exceeding substantial switching costs in the customer base.

Classifying Security Lock-In

We can classify types of security lock-in into several broad categories:

- Proprietary Security Protocols
- Open Security Protocols
- Proprietary Extensions to Open Security Protocol
- Intellectual Property Rights and Other Legal Constructs

Proprietary Security Protocols

In this type, a proprietary security protocol or architecture is a potential source of lock-in. There are numerous examples of this class, including set-top boxes in the cable industry (further developed in a subsequent section), wireless communication protocols, and hardware and software rights management for the PC.

In the case of wireless access devices, Cisco's LEAP products make use of proprietary security extensions applied to 802.11 (an open and very successful wireless LAN standard also known as Wi-Fi). The argument put forth for this proprietary development was that the existing wireless LAN security mechanisms were far too weak to promote adoption by security concerned consumers.

The Trusted Computing Platform Alliance (TCPA), an initiative led by Intel and assisted by Microsoft, proposes to create "a new computing platform for the next century that will provide for improved trust in the PC platform". However, critics claim that it is the application of hardware and software security technologies to not only restrict the distribution of copyright materials, but also to lock users into software suppliers. While the Digital Rights Management (DRM) issue is a clear and specified goal, it is the potential for this technology to restrict users from deploying competing software that raises some concern. While avoiding the detail, the argument is that a supplier would have to comply with a certification process potentially developed by Microsoft, which might be burdensome or potentially anticompetitive.

The use of proprietary security to preclude manufacturing of low cost clone components is particularly relevant in industries which adopt a "razor and blades" pricing strategy. In these cases a central component may be provided at unusually low margins, even at a loss, with the expectation that a customer will become locked-in via the purchase and subsequently buy a sufficient quantity of higher margin cartridges to make the overall

relationship profitable to the supplier. Apparent examples of the use of encryption in these cases to enhance lock-in include the printer industry (the previously discussed Lexmark case) and the video game industry, in which a number of suppliers have used proprietary security mechanisms to control the access of game cartridges to those licensed by the video game console manufacturer (beginning apparently with the Atari 7800 in the 1980's).

Open Security Protocols

A supplier might make use of standard (open) security protocols to prevent competitors from developing interoperable software or hardware components. As with the case of proprietary security protocols, the video game industry also uses open security protocols to prevent unauthorized game cartridges – for example, the use of private key cryptography to sign cartridge software in the Microsoft X-box. The cable industry also uses public key cryptography so that set top boxes require authentication mechanisms provide via PKI certificates to operate. These certificates are obtained after verification testing by a supplier, a potentially lengthy and costly procedure.

Proprietary Extensions to Open Security Protocols

Proprietary extensions of an existing open security protocol may prevent interoperability with other standard compliant software and become a source of lock-in. Microsoft, for example, has had a stated objective of 'embracing, extending and extinguishing' (to paraphrase Paul Maritz) standardized protocols in this manner. In the case of security protocols, in the late 1990s, Microsoft created a proprietary extension to the Kerberos authentication protocol. This extension tied the Kerberos client software to the Windows 2000 Server and integrated an authorization process into the mechanism, thereby making it difficult to interoperate with other servers. Microsoft pursued a similar extension in its development of Passport, its solution for single sign-on web based services. Here again, Microsoft proposed extensions to existing protocols, but in this case to tie the customer to a web services platform. This mechanism also created much debate in the privacy community, with concerns surrounding one entity potentially being aware of a user's web behavior and shopping history. Other suppliers have extended protocols such as Secure Shell (SSH) and security related Session Initiation Protocols (SIP).

It may be that this is becoming a defining characteristic of competition in high technology industries with strong network effects – as these can lead to high concentration among suppliers (and hence substantial market power) yet exhibit high interest in compatibility to drive the overall growth of such industries (hence an interest in standardization). A standard tactic of market dominant players may be, when embracing open standards, to extend a protocol just sufficiently to preclude certain aspects of interoperability with competitors. Security protocols may not be privileged over other technologies in this respect but can be expected to play a role.

Intellectual Property Rights and Other Legal Constructs

This is a rather abstract case, in that it is not the security protocol itself that creates the lock-in, but rather the application of intellectual property rights around this technology. To illustrate this class, consider a company that establishes a security technology and then charges a licensing fee for its use. A prime example is that of the RSA algorithm.

For many years, RSA (the company) charged fees for the use of RSA technology, but recently released this requirement ahead of the patent expiration. Recent IPR debates surrounding web services technology such as Shibboleth suggests that these relatively pure intellectual property versions of security based lock-in will likely continue.

To avoid overlap, the classifications we describe above are purposely broad. In fact, there are a number of possible distinctions we might have presented. For example, finer analysis could be developed along the lines of hardware versus software or device based versus network based. While such an analysis may ultimately be useful, it could also create confusion due to the potential overlap that would exist within the examples. The point that we are trying to make is that there are indeed a number of such potential lock-ins.

As the above classifications suggest, suppliers have long benefited from security as a lock-in measure. Many of these measures have been rooted in legitimate security mechanisms (or, more skeptically, may have been disguised as such) developed for such needs as authentication, authorization and privacy. However, all of the above implementations create an opportunity for lock-in.

The U S Cable Industry

The U S cable industry's purchase of set-top boxes represents a particularly rich example of security based lock-in. Although to date we have collected primarily anecdotal evidence of the various aspects of security based lock-in in the cable industry, we are currently collecting more comprehensive quantitative and qualitative data.

The U. S. cable industry purchases set-top boxes and uses them to provide its subscribers with access to programming. Over the last decade, the industry has increasingly been deploying digitally based set-top boxes to replace analog ones. The cable operators buy their set-top boxes almost exclusively from two suppliers, Motorola (which purchased the former General Instrument) and Scientific Atlanta. Each supplier maintains a proprietary conditional access (rights management) system and the programming provided in each cable operators' cities is compatible with the conditional access system of one or the other supplier. Consequently, the cable operators are locked-in in each city to one of the two suppliers; the switching cost for a non-compatible alternative would include replacing all currently deployed set-top boxes in that city plus a substantial portion of the network equipment that processes programming (typically called "head end" equipment).

Anecdotal evidence regarding the choice of set-top suppliers and the existence of lock-in suggests the following:

i) Cable operators perceive themselves as locked-in and are aware of the consequences. They actively pursue strategies to reduce the effect of lock-in, but have not been successful to date in substantially reducing the effects. Their current initiatives revolve around licensing (either direct or via creation of a removable security module) but appear likely to satisfy the expectation that their suppliers will retain the profit of lock-in via licensing prices.

ii) There are examples of different product pricing trends in similar, less locked-in technologies both outside the cable industry (DVD players) and inside (cable modems).

iii) The cable industry has shown evidence of anticipating the price impacts of lock-in and negotiating up front compensation. For example, industry leader John Malone negotiated substantial feature, price, and other concessions from General Instrument during a seminal deal that locked his company TCI into General Instrument's product several years ago. However, industry leaders currently believe that they underestimated the impact of lack of access to innovation and that this has had competitive consequences relative to the satellite television industry and consequences in terms of opportunities lost relative to innovations introduced in the more general consumer electronics industry.

iv) Security has played a privileged role in lock-in. Although both suppliers started with a number of other proprietary technologies, including video processing, modulation, and audio processing, that could have been the locus of lock-in, only security remains as a clear source of proprietary lock-in, the others having yielded to open standards or solutions licensed from third party suppliers accessible to all suppliers (both current and potential).

Implications

The previous section suggests that many aspects of security induced lock-in actually do occur in practice, though the specific mechanisms and their import substantially vary by case. Nonetheless, the existence of security induced lock-in suggests a number of possible initiatives depending on the role a party plays: customer, supplier, or policy maker.

Customers

Lock-in can arise as a mutually beneficial state for both customer and supplier. Some types of lock-in (such as a customer investment in supplier specific training) do increase switching costs but at the same time may increase customer profit via improved efficiency even more than the implied shift in profit to the supplier. In other cases, particularly where customers and suppliers are both concentrated, bi-lateral lock-in may occur in which the supplier is also locked-in to the customer, would experience substantial switching costs in pursuing another customer, and is therefore induced to make concessions to the customer. Bi-lateral lock-in may be a less colorful but more precise statement of what it really means for a customer and supplier to "partner."

Nonetheless, Shapiro and Varian advance a simple but useful rule of thumb that the customer's switching cost equals the net present value of a supplier's profit in excess of what they could earn on the basis of the competitive strength of its product in the absence of lock-in [16]. So, a customer is normally interested in reducing switching cost and a supplier in increasing them. Here we suggest a number of strategies, some specific to security.

1. Estimate impact of lock-in on access to innovation and include in negotiated up front concessions. There is no particular recipe to how to do this but rather an admonition to

try. More practically, it may be feasible to negotiate clauses that will force access to innovation if such innovation occurs, e.g., by triggering licensing of security protocols to other suppliers on pre-negotiated terms.

2. Consider open security systems. This amounts to rejecting the “security by obscurity” approach. Customers may be able to find existing open security standards that one or more suppliers will implement, or if sufficiently concentrated may be able to leverage an industry consortium to establish such a standard. A next best alternative would be to cause suppliers to license security technology from a third party. Of course, this creates lock-in to the third party, but if that supplier has less ability to use security in tying sales of products together, this may be a less expensive proposition. A related initiative in the case where a customer has a great deal of market power would be to attempt to restructure the supplier industry so that security is captured in a third party organization, for example, by forcing a potential supplier to divest its security technology component into a separate company.

3. Develop credible commercial alternatives. This is a normal attack on lock-in. Investing in enabling another supplier implicitly lowers switching costs. The critical question is whether switching costs are lowered more than the investment, and whether the value can be realized reasonably quickly through continuing negotiations with the incumbent supplier. Simultaneously, the interest of an alternative supplier in participating, particularly if it is also making its own investments in support of the process, will be dampened if it perceived that it is only being used as a stalking horse (i.e., although the customer may realize a commercial advantage from the strategy, the alternative supplier never does).

4. Developing or selecting technical and architectural alternatives that weaken the effect of lock-in. There may be options that are different from adoption of an open standard. For example, selective encryption has been proposed as a technological solution in the U.S. cable industry. It allows the introduction of a second conditional access system overlaid on an existing one without requiring replacement of the installed base of set-top boxes, albeit at some overhead in transmission bandwidth [5].

Suppliers

Since suppliers typically benefit from lock-in, most strategies should either aim to increase it or decrease the incentive for customers to attempt to reduce it.

1. Enhancing arguments for the added value of proprietariness in security systems. This implies supporting the “security by obscurity” argument. A reasonable variant to advance (and one that is frequently used in conditional access systems) is “defense in depth.” In this approach, a security system has multiple secret “fall backs” that are used to increase the cost or reduce the impact of breaches [2].

2. Embedding security as a component in a rich collection of lock-in devices (e.g., other proprietary technologies, customer training investments, relationships) so that it is difficult to isolate it and reduce its impact. Particularly potent in information technology is lock-in that derives from network effects; lock-in driven by mutually supportive network effects and security technology is likely to be particularly effective.

3. Seek a compromise in which some potential lock-in profit is reduced but access to innovation is increased, in particular:

- Increased internal spending on innovation.
- Voluntary and attractive licensing terms or integration efforts to provide customers with access to innovations developed by others.

The goal here is to spend less on these initiatives than would be lost if the customer seriously incubated alternative suppliers in order to access innovation, and in particular to avoid the worst case of replacement as part of a process of serial lock-in.

Policy Makers

Policy makers have a number of options. To the extent security induced lock-in has resulted in convergence to a stable equilibrium that is not the globally optimal one (from the overall societal welfare perspective), policy makers should be interested in strategies to weaken the lock-in, providing, of course, that the medicine prescribed is not worse than the disease. Options include:

1. Regulation. Policy makers can directly regulate the use of security technologies with a goal to avoiding their use in lock-in. Conversely, they may, intentionally or not, increase the role of security in lock-in, as arguably has occurred with the Digital Millennium Copyright Act.

2. Antitrust Actions. Some versions of lock-in are caused by or associated with activities that are illegal under antitrust law and the use of security technology may be involved (for example, if it facilitates illegal tying). In these cases, policy makers can pursue antitrust remedies.

3. Support for Standards. The government has a successful history of supporting certain key security standards (e.g., DES and AES). Some challenges exist, though, in internal tensions between desire to promulgate good security, and the concerns of military intelligence and law enforcement branches that would prefer that security not be too strong to preclude wiretapping. A broadened role in either directly driving security technology standards or in creating a favorable environment for consortia and other bodies to develop security standards will tend to reduce the role of security in lock-in.

4. Nothing. Under the “first do no harm” maxim, government can rely on the increasing sophistication of customers to correctly anticipate security based lock-in and either secure the appropriate compensation or themselves develop initiatives to reduce the lock-in.

References

1. Student pleads guilty in DirecTV data case *Associated Press*, 2003.
2. Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., New York, 2001.
3. Anderson, R., Security in Open versus Closed Systems - The Dance of Boltzmann, Coase, and Moore. in *Open Source Software: Economics, Law and Policy*, (Toulouse, France, 2002).

4. Arthur, W.B. *Increasing Returns and Path Dependence in the Economy*. The University of Michigan Press, Ann Arbor, MI, 1994.
5. Baumgartner, J. Deciphering the CA Conundrum *Communications Engineering and Design*, 2003.
6. Kamien, M. and Schwartz, N. *Market Structure and Innovation*. Cambridge University Press, Cambridge, UK, 1982.
7. Kerchoffs, A. La cryptographie militaire. *Journal des sciences militaires*, IX. 5-38.
8. Liebowitz, S.J. and Margolis, S.E. *Winners, Losers & Microsoft*. The Independent Institute, Oakland, CA, 1999.
9. Lipner, S.B., Security and source code access: issues and realities. in *IEEE Symposium on Security and Privacy*, (Oakland, CA, 2000).
10. Neumann, P.G., Robust Nonproprietary Software. in *IEEE Symposium on Security and Privacy*, (Oakland, CA, 2000).
11. Nowell, P. Small firm irks printer giant; cartridges at center of legal tussle *The Seattle Times*, Seattle, WA, 2003.
12. Redding, S. Path Dependence, Endogenous Innovation, and Growth. *International Economic Review*, 43 (4). 1215-1248.
13. Scherer, F. Changing perspectives on the firm size problem. in Acs, Z. and Audretsch, D. eds. *Innovation and Technological Change: An International Comparison*, The University of Michigan Press, Ann Arbor, MI, 1991, 24-38.
14. Schneider, F.B., Open source in security: visiting the bizarre. in *IEEE Symposium on Security and Privacy*, (Oakland, CA, 2000).
15. Schneier, B. Open Source and Security *Crypto-Gram Newsletter*, 1999.
16. Shapiro, C. and Varian, H. *Information Rules: A Strategic Guide to the Network Economy*. Harvard Business School Press, Boston, MA, 1998.