Revisiting the Incentive to Tolerate Illegal Distribution of Software Products

Atanu Lahiri
lahiria@uw.edu
Foster School of Business
University of Washington

Abstract

Motivated by the recent strategy switch of a large software producer, this paper revisits the tradeoffs associated with tolerating illegal distribution of software products. Conventional wisdom is that a higher level of positive network effects justifies a tolerant approach on the part of software producers — because illegal distribution leads to more users, amplifies positive network effects, and creates a greater demand for the legal version. I show that this wisdom does not hold in the context of supporting illegal versions with patches. Patches are used for plugging security vulnerabilities as well as for distributing functionality changes. Software producers have the option of supporting illegal versions with either or both kinds of patches. I find that a higher level of positive network effects surprisingly requires the least tolerant approach of denying illegal versions both kinds of patches.

Keywords: Distribution Channels for Information Goods, Network Effect, Software Piracy, Software Security and Patching, Fulfilled Expectations Equilibrium

1. Introduction

In the US, 22 percent of personal computer users use illegal copies of the Windows system; in absolute terms, a staggering 12 million users in this country use illegal copies of the Windows [7]. Another 13 million illegal copies are in use in China [7]. We need to add to this number the number of illegal copies floating in all other countries to get an estimate of the total number of illegal copies and the lost revenue; the lost revenue in Microsoft’s case is clearly several billions, if not tens of billions. Simply put, piracy, for many software products, results in a severe cannibalization of the legal demand and adversely impacts profits of software manufacturers.

Piracy problem is often exacerbated by illegal retailers who sell illegal copies at significant discounts vis-à-vis suggested retail prices of original products. These illegal retailers often have excellent understanding of the markets they operate in, and are very effective in convincing consumers about the economic benefits of acquiring software and other services from them. The existence of this parallel illegal distribution channel makes piracy a very difficult problem to deal with. Software manufacturers thus constantly have to look for technologies, legal recourses, and other means (some common approaches are listed in §2) to contain this channel.

To curb piracy software manufacturers typically use a combination of strategies including the Digital Rights Management or DRM technology. Existing research on DRM shows that the manufacturer makes larger profits by tolerating piracy if positive network effects are sufficiently large [5]. The existing research however does not explain whether this relationship between the incentive to tolerate piracy and positive network effects is applicable to other important contexts such as the context of patching. Consequently, the existing research does also not explain why Microsoft, despite benefiting from large positive networks effects, in recent years has stopped offering certain software patches to illegal users.

So, what are these patches? Patches are essentially changes to the original software. The
changes can be functionality related, security related, or a combination of the two. At times the changes are offered individually, at other times they are combined into “service packs.” These days software patches are frequently distributed using the Internet. For instance, Microsoft makes patches for the Windows operating system available through the tool called “Microsoft Update.” If a user has the “automatic update” feature turned on, she receives patches automatically as soon as she goes online the very first time on or after the second Tuesday of any month (or the very first time after the release of a new patch). Alternatively, any user can visit the Microsoft Update site periodically to download and install critical patches. Patches are also common for other software manufacturers and for other types of software. As of August 2006, Apple provided 45 patches for “Panther” (10.4) version of its operating system. And, Adobe updated its Acrobat 7 product on average once every 89 days.

What then makes patching a viable instrument for controlling piracy? The answer, in short, is the Internet. The Internet not only serves a channel for patch distribution, it also allows for two way communication that can be used by a software manufacturer to authenticate installations seeking patches. Common authentication techniques rely on unique keys, system signatures and a database of authentications. Such techniques can easily identify installations that do not meet the End User License Agreements (EULA). Microsoft’s “Genuine Advantage” is an example of one such tool that validates installations prior to patch distribution. Armed with such tools that can distinguish between legal and illegal installations, a software manufacturer can limit distribution of its patches to legal installations, thereby creating a “quality gap” or a vertical differentiation between the legal and illegal (pirated) versions of its product. This quality gap reduces the cannibalization of the legal demand by piracy. It is useful to note here that patches are distributed frequently using the Internet, which makes stealing patches almost impossible. Further, as I argue later, for most patches, timely deployment is critical, which means that patches received from illegal sources well after their original releases would be almost worthless. Hence, the manufacturer remains in control of its patch distribution, and retains the ability to influence piracy by denying illegal versions certain patches.

It is certainly tempting to think that the value of containing illegal distribution is minimal when the level of positive network effects is large, because reducing piracy can shrink the user base and significantly lower positive network effects [5]. However, the recent strategy switch of Microsoft indicates that exactly the opposite may be true. In 2004, Microsoft decided to provide the Service Pack 2, a major compilation of security and functionality upgrades to its existing Windows XP product, to all users, legal and illegal alike. However, Microsoft has since changed its patching strategy. According to an Associated Press report [1], Microsoft is now following a policy of offering critical security fixes to all users while restricting feature enhancements and functionality related fixes only to authenticated copies. Specifically, Microsoft no longer offers feature updates to Internet Explorer, Windows Media Player, or Windows Defender to illegal installations though it still offers security updates to its Windows system to all users.

Microsoft’s decision is an interesting one, and is driven by economic considerations. Microsoft, or any software manufacturer for that matter, has four possible policy choices: (PN) offer pirates nothing, (PF) provide pirates only functionality patches/enhancements, (PS) provide pirates only security fixes, and (PA) provide pirates all patches. First, consider the choice of offering feature enhancements or functionality related fixes to pirates. If users of pirated copies have lesser access to these enhancements and fixes, the quality of their product will be lower than that of the legal product, i.e., the pirated version would suffer from a “functionality gap.” This functionality gap works as an added incentive to prefer the legal product. However, as I have already mentioned, positive network effects, which are exhibited by most software products, complicate this consideration.
What about security related fixes? Not offering these fixes makes pirates more vulnerable to security threats, i.e., makes the pirated version suffer from a “security gap.” While this gap discourages piracy, not securing illegal copies also results in a larger pool of vulnerable machines in the network. A larger vulnerable pool offers a breeding ground for virus, worms, etc., and can also become a zombie for denial of service (DoS) attacks. This makes the network less secure, and reduces the value of the software to all legal and illegal users [2]. August and Tunca [2] are among the first to model this negative network effect. However, they do not consider positive network effects, and, as a result, do not explain what happens when both network effects are simultaneously present.

One may ask why legal users, who have access to patches, should worry about increased security threats. Many legal users, particularly businesses, have their own processes for testing and distributing patches. Such processes often delay application of critical patches. For example, a corporation may choose to patch its non-critical computers first to test the quality of a patch. Also, patching can interfere with day-to-day activities of these corporations or individuals [9]. A small business owner may delay application of a patch if application of the patch involves rebooting of its computers and disruption of some time-critical tasks. Such delays create a window of opportunity between the release of a patch and its actual application, which worm-attackers love to exploit. Consider, for example, the Zotob worm attack, which was launched within a day of the release of the relevant patch and the disclosure of the associated vulnerability [6]. Previous worms such as Sasser, Blaster or Code Red were launched weeks or months after disclosures of corresponding vulnerabilities. Big corporations, most notably the media conglomerates, were completely overwhelmed by the speed of the Zotob attack — all these corporations patched, but they did not patch fast enough. Since “zero day exploits” like the Zotob worm are becoming increasingly common, I hypothesize that even users of legal copies, regardless of their willingness to patch, are affected by vulnerable pirated copies (because vulnerable pirated copies increase the possibility of infection in the presence of patching delays, and also increase the likelihood of DoS and other malicious attacks on the network). In my model, this negative network effect, which is present even when all legal users are willing to patch, lowers the value of the software product to legal users. It is worth noting that some pirates may not apply patches timely and that giving them patches therefore may not improve network security. However, as long as some pirates apply patches promptly, giving patches to pirates makes the network more secure on the margin. My model focuses on this marginal improvement and its impact on profits, and not on network security in an absolute sense.

The rest of this paper is organized as follows. I first discuss the related literature. Next, I present my model. Using numerical examples, I then examine how different levels of positive and network effects affect the equilibrium profit. I conclude by summarizing main contributions and limitations of my work.

2. Literature

This chapter is related to different streams of literature. One key stream is the economics of networks. Katz and Shapiro [8] examine the role of positive network effects in the context of competition and technology choice using the notion of Fulfilled Expectations Equilibrium. Conner and Rumelt [5] apply the same notion to analyze the monopolist’s incentive to tolerate piracy in the presence of positive network effects. Conner and Rumelt [5], however, do not consider negative network effects, which I closely examine here. I show that the incentives to tolerate piracy are very different in the presence of negative network effects.

Another key stream is the economics of managing piracy. Shy and Thisse [10] present the possibility of bundling support with purchase as a strategy to counter piracy. It compares the strategy of bundling support with purchase with the strategy of employing DRM technologies. One of the interesting findings is that,
in the presence of positive network effects, the strategy choice depends on the value of support. Chellappa and Shivendu [4] discuss the possibility of offering free trials to curb piracy of digital experience goods whose value cannot be understood without trials. Sundararajan [11] analyzes the implications of piracy on software pricing. Wu et al. [12] discusses the possibility of fighting piracy by offering cheaper stripped down versions to price-sensitive consumers. I here focus on using patch distribution as a mechanism to manage piracy.

My work is also related to the work on negative network effects that arise from not offering security fixes to pirates [2]. Unlike August and Tunca [2], I allow dual network effects, i.e., I consider both positive and negative network effects. Additionally, I consider both functionality enhancements and security fixes, and also explicitly model the heterogeneity in piracy costs, which include costs associated with procuring an illegal copy as well as potential legal liabilities.

Since I address the role played by the quality gap (between legal and illegal versions) in deterring piracy, my work is also closely related to the work on vertical differentiation. Bhar-gava and Choudhary [3] provide insights into the monopolist’s vertical differentiation problem — in their model, the monopolist decides the number of versions to offer. On the contrary, in my model, the lower quality version is the pirated version and the manufacturer does not control the decision to offer it. However, the manufacturer can influence the quality of the lower version, i.e., that of the pirated product, by employing different patching strategies.

3. Model
My model assumes the following time line. The software manufacturer, who is presumed to be a monopolist facing a zero marginal cost, first chooses the patch policy and the price. Then, each potential user decides whether to purchase a legal copy, or to procure an illegal copy, or to forgo the use of the product completely. The manufacturer and potential users base their decisions on their expectations regarding the sizes of the legal and illegal markets. At the Fulfilled Expectations Equilibrium, their expectations are realized. The equilibrium demand determines the monopolist’s revenue. Note that, because I assume a zero marginal cost, I use the terms “revenue” and “profit” interchangeably.

Let the utility of the legal copy to a potential user be \( e_l x - p \), where \( e_l \) is the quality of the legal copy (throughout the paper I use the subscript \( l \) for legal and \( i \) for illegal), \( x \) is the intrinsic value of the software (the value of the software to the user in the absence of all network effects), and \( p \) is the price. Let the utility of the illegal copy be \( e_i x - y \), where \( e_i \) is the quality of the illegal version and \( y \) is the cost of piracy faced by the user. Therefore, the user, characterized by the tuple \((x, y)\), buys the legal version if the following Individual Rationality (IR) and Incentive Compatibility (IC) conditions are satisfied:

\[
\begin{align*}
e_l x - p & \geq 0 \quad \text{(IR)} \\
e_l x - p & \geq e_i x - y \quad \text{(IC)}
\end{align*}
\]

Similarly, the user buys the illegal version if the following conditions are satisfied:

\[
\begin{align*}
e_i x - y & \geq 0 \quad \text{(IR)} \\
e_i x - y & \geq e_l x - p \quad \text{(IC)}
\end{align*}
\]

3.1. Quality Factors
The quality factors, \( e_l \) and \( e_i \), depends on the software maker’s patching strategy as well as the expected sizes of the legal and illegal markets, which equal the realized sizes in the equilibrium. I denote the equilibrium sizes of the legal and illegal markets by \( q_l \) and \( q_i \), respectively. I denote the total demand by \( q \), i.e., \( q = q_l + q_i \). I denote the software maker’s patching strategy by \( I \), which is one of the four described earlier, i.e., \( I \in \{PN, PA, PS, PF\} \). The relationship between the quality factors and patching strategies is as described by the following four assumptions.

Assumption 1. If all patches are offered to pirates, i.e., \( I = PA \), pirates and legal users
are assumed to enjoy the same quality. Specifically, \( e_i = 1 + e(q_i) \), where \( e(q) \), the positive network effect, is a non-decreasing function of \( q \) and \( e(0) = 0 \). The function \( e(.) \) is common knowledge.

**Assumption 2.** If only security fixes are offered to pirates, i.e., \( I = PS \), \( e_i = 1 + e(q) \) and \( e_i = 1 + e(q) - \beta \), where \( 0 \leq \beta < 1 \) represents the “functionality gap.” \( \beta \) is common knowledge.

The assumption that \( e(.) \) or \( \beta \) are common knowledge is similar to what we find in the existing literature [5]. For example, most users can correctly anticipate that \( e(.) \) is larger for a word processing software than it is for a disk de-fragmentation software. Similarly, users often know in advance what patches make up \( \beta \); e.g., for Windows system, it is made up of feature updates to the Internet Explorer browser, the Windows Media player, and the Windows Defender tool. Also, since \( \beta \) is not related to security concerns that arise from leaving certain users insecure, I assume that it does not depend on \( q_i \) or \( q \).

**Assumption 3.** If only functionality changes are offered to pirates, i.e., \( I = PF \), illegal users face an equal or bigger security risk even though all users suffer a loss in value due to negative network effects. Specifically, \( e_i = 1 + e(q) - \alpha(q_i) \) and \( e_i = 1 + e(q) - \alpha(q_i) - \delta(q_i) \), where \( \alpha(q_i) \) represents the negative network effect (the common loss in value arising from pirates not having access to security patches) and \( \delta(q_i) \) represents the “security gap.” Both \( \alpha(q_i) \) and \( \delta(q_i) \) are non-decreasing in \( q_i \), and \( \alpha(0) = \delta(0) = 0 \). Further, \( \alpha(.) \) and \( \delta(.) \) are common knowledge.

**Assumption 4.** If no patches are offered to pirates, i.e., \( I = PN \), both the “functionality gap” and “security gap” separate the legal and illegal versions. Specifically, \( e_i = 1 + e(q) - \alpha(q_i) \) and \( e_i = 1 + e(q) - \alpha(q_i) - \delta(q_i) - \beta \).

The assumption that \( \alpha(.) \) and \( \delta(.) \) are common knowledge may appear to be a strong assumption in the sense that users may find it hard to anticipate security threats. Yet, such assumptions have been used in the literature [2]. They are also not unreasonable in the sense that potential users may be able to estimate — based on the software maker’s reputation or by looking at its other products — the impact of likely security threats, and thus they may be able to anticipate \( \alpha(.) \) and \( \delta(.) \).

Further, \( \alpha(q_i) \) and \( \delta(q_i) \) have been assumed to be functions of \( q_i \), the number of illegal users. The reason is that \( \alpha(q_i) \) provides a measure of the “additional” security concerns that legal users face when illegal users are not given security patches. Similarly, \( \alpha(q_i) + \delta(q_i) \) is a measure of the “additional” security concerns that illegal users face. Since \( \delta(q_i) \geq 0 \), my assumptions imply that illegal users are on the margin at least as insecure as are legal users, which is reasonable since legal users remain vulnerable until they patch while illegal users remain vulnerable for a longer period. Further, my assumption that \( \alpha(q_i) \) and \( \delta(q_i) \) are functions of \( q_i \) does not rule out the possibility that they can be constants. For example, \( \delta(q_i) = \tilde{\delta} \), where \( \tilde{\delta} > 0 \), would just be a special case of my model.

### 3.2. Fulfilled Expectations Equilibrium

In a Fulfilled Expectations Equilibrium, the number of users is endogenously determined. I can normalize the market size to 1 without loss of generality. Let \( x \), the intrinsic value, and \( y \), the piracy cost, be independently distributed with distribution functions \( F(x) \) and \( G(y) \), respectively. I also assume that these distribution functions are publicly known. However, only each user is assumed to be aware of his own value for \( x \) and \( y \). The IR and IC conditions above then imply that:

\[
q_i = \int_{p/e_i}^{\infty} \int_{p - (e_i - e_i)x}^{\infty} dG(y)dF(x) \tag{1}
\]

\[
= 1 - F(p/e_i) - \int_{p/e_i}^{\infty} G(p - (e_i - e_i)x)dF(x)
\]

Examining the number of legal users, \( q_i \), it consists of two parts. The first part, \( 1 - F(p/e_i) \), is the demand if the price is \( p \) and piracy is not possible. This is reduced by the last term, which is the cannibalization of legal demand by piracy.
Let me denote this cannibalization quantity by $q_c$.

$$q_c = \int_{p/e_l}^{\infty} G(p - (e_l - e_i)x) dF(x)$$

The IR and IC conditions also imply that:

$$q_i = \int_{0}^{p/e_l} \int_{e_i x}^{\infty} dG(y) dF(x)$$

$$= \int_{0}^{p/e_l} G(e_i x) dF(x)$$

$$+ \int_{p/e_l}^{\infty} \int_{p-(e_l-e_i)x}^{\infty} dG(y) dF(x)$$

Hence, there are two categories of illegal users: one who are submarginal with respect to price, and their number is represented by the first term above, and another who give up the legal version in favor of the pirated copy, and their number, $q_c$, has been defined above.

The equilibrium is characterized by the above pair of simultaneous equations in $q_l$ and $q_i$, i.e., equations 1 and 2. Note that the right hand side of each equation is also a function of $q_l$ and $q_i$ because $e_l$ and $e_i$ depend on $q_l$ and $q_i$. Solving these two equations for a given patching strategy, we can obtain $q_l$ as a function of the price, $p$. The carrier’s problem for a given patching strategy is to then maximize $pq_l$. The strategy that leads to the highest maximum value for $pq_l$ is what I refer to as the optimal patching strategy.

4. Numerical Experiments

The equilibrium is not easy to solve in the closed form without making further simplifying assumptions. However, a great deal of insights can still be obtained from my model using numerical experiments, which I present in this section.

The examples shown in Figures 1 and 2 assume the following forms for the network effect and security gap functions: $\alpha(q_i) = \alpha q_i$, $\delta(q_i) = \delta q_i$, and $e(q) = eq$, where $\alpha$, $\delta$, and $e$ are positive constants. Further, they assume that the distribution of the intrinsic value ($x$) is uniform over $[0, 2]$, and the distribution of the cost of piracy ($y$) is uniform over $[0, 1]$ (assuming both to be distributed uniformly over $[0, 1]$ leads to similar results; but assuming identical distributions is not necessary). Recall that, for each strategy, I must first solve $q_l$ for different values of the price, $p$, in order to find out the profit at different price levels for that strategy; only then I will be able to compare different strategies.

Figures 1 and 2 show how, for two different sets of parameter values, the equilibrium profit varies with respect to the price for different patching strategies. Parameter values assumed for each figure are as mentioned below the figure. To compare the strategies for any figure, I need to look at the maximum profit for each strategy, i.e., I need to compare the peaks of the profit curves.
In both figures PS, which is Microsoft’s current strategy for its Windows Vista and 7 systems, outperforms PA, which was Microsoft’s strategy for its Windows XP system; i.e., the peak of the profit curve for PS is higher than that for PA. Further, PF and PA turns out to be dominated in both situations, which is also consistent with Microsoft’s move to PS.

Interestingly, PN outperforms PS in Figure 2 but PS outperforms PN in Figure 1. Note that the two figures assume identical parameter values except that Figure 2 assumes a higher level of positive network effects (i.e., a higher value for $e$). These two figures thus indicate something surprising, that a strong positive network effect does not justify a more piracy-friendly approach. As is depicted by these two figures, a higher level of $e$ may in fact require a more restrictive approach, which contradicts the findings of Conner and Rumelt [5].

Since my model has both network effects, it also allows us to examine the impact of different levels of positive network effects at different levels of negative network effects. Table 1 shows how optimal profits for different strategies compare for different combinations of $\alpha$, the level of negative network effects, and $e$, the level of positive network effects. The table continues to assume the same parameter values for the other parameters, i.e., it assumes that $\beta = 1/8$ and $\delta = 1/8$. The optimal strategy for each combination of $\alpha$ and $e$ is shown in bold.

There are two things that we can immediately infer from the table: one is that a higher level of negative network effects (i.e., a larger $\alpha$) increases the attractiveness of PS, and the other is that a higher level of positive network effects (i.e., a larger $e$) increases the attractiveness of PN. Therefore, near the right-top corner of the table, the optimal strategy is PS. But, as we move towards the left-bottom corner, the optimal strategy becomes PN.

The fact that a larger $\alpha$ requires PS is not very surprising; it confirms our intuition that not securing illegal copies in the network can substantially lower the legal demand when negative network effects are large. Therefore, securing illegal copies becomes preferable to not securing them. However, what is counterintuitive is that a higher level of positive network effects in this case requires PN, the least piracy-friendly approach. As we know from the existing literature [5], a higher level of positive network effects usually requires pursuit of strategies that lead to a larger user base, including strategies that lead to more illegal users.

I now explain why my results regarding positive network effects differ from those in the literature. As already mentioned, Conner and Rumelt [5] focus on DRM. The primary effect of DRM is on costs involved in procuring an illegal copy. When piracy costs go up, some pirates forgo the use of the software product and the user base shrinks. When the level of positive

![Figure 2. Profit vs. Price for $\alpha = 3/2$, $\delta = 1/8$, $\beta = 1/8$ and $e = 2$](image)
Table 1. Optimal profit for $\delta = 1/8$ and $\beta = 1/8$

<table>
<thead>
<tr>
<th>$\epsilon$</th>
<th>PN: 0.271</th>
<th>PS: 0.267</th>
<th>PF: 0.214</th>
<th>PA: 0.209</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.50</td>
<td>PN: 0.279</td>
<td>PS: 0.274</td>
<td>PF: 0.224</td>
<td>PA: 0.214</td>
</tr>
<tr>
<td>0.75</td>
<td>PN: 0.283</td>
<td>PS: 0.279</td>
<td>PF: 0.229</td>
<td>PA: 0.218</td>
</tr>
<tr>
<td>1.00</td>
<td>PN: 0.292</td>
<td>PS: 0.279</td>
<td>PF: 0.232</td>
<td>PA: 0.218</td>
</tr>
<tr>
<td>1.25</td>
<td>PN: 0.299</td>
<td>PS: 0.283</td>
<td>PF: 0.238</td>
<td>PA: 0.222</td>
</tr>
</tbody>
</table>

network effects is large, this shrinkage translates to a large drop in legal users’ willingness-to-pay for the product. As a result, the equilibrium demand curve shifts inwards, which invariably leads to lower profits.

On the contrary, denying pirates patches primarily impacts the gap between the legal and illegal versions of the product, and it converts pirates into legal users. It is true that lowering the quality of the illegal version shrinks the user base. However, that shrinkage is only a secondary effect. The primary effect of managing piracy through strategic patching is on the cannibalization quantity. In fact, strong positive network effects can substantially drive up the overall demand (i.e., the total demand for the legal and illegal versions). When the total demand is high, it becomes necessary to ensure that this demand also translates to a higher demand for the legal copy. As I show here, one way to do that is to employ extremely restrictive patching strategies such as PN.

Coming back to Microsoft’s situation, there are two possibilities: (a) its Windows system experiences a high $\alpha$, making PS the optimal choice, or (b) the Windows system experiences a higher $\epsilon$ vis-à-vis $\alpha$, making PN the optimal choice, but Microsoft still uses PS to avoid any negative publicity and public scrutiny that are likely to result from malicious attacks on computers running the Windows software. As is evident from the experiments above, PA does not seem an attractive option, which is perhaps why Microsoft no longer considers it an alternative. Interestingly, Table 1 shows that, both the gap between PN and PA and the one between PS and PA widen as $\epsilon$, the level of positive network effects, increases. PA therefore appears to be an unlikely choice for any software maker whose products benefit from strong positive network effects.

5. Conclusion

In this paper I examine whether a software producer can benefit by offering certain patches free of cost to illegal users of its product, and, specifically, whether doing so is an attractive option when positive network effects are strong. Offering security related patches to illegal users certainly makes the network more secure and increases legal users’ willingness-to-pay for the product. But, doing so reduces the incentive to prefer the legal version to the illegal version. Offering functionality related patches also reduces the incentive to buy the legal version, but doing so contributes to the user base and positive network effects. In short, offering either
kind of patches free of cost to illegal users has its own upsides and downsides. I examine a model in which these two intertwined trade-offs are present simultaneously. Using my model, I study the equilibrium demand and optimal profit for each strategy.

The salient contribution of this work is that it explains why, contrary to the common wisdom, stronger positive network effects may require a less piracy-friendly and a more restrictive patching strategy of not offering any patches to pirates. It shows that strategic patching and DRM are very different approaches to managing piracy. DRM and strategic patching both reduce piracy. But DRM raises costs of piracy, which makes some illegal users forgo the use of the product, shrinking the overall user base in the process. A smaller user base fails to leverage high levels of positive network effects, and, as a result, it often means lower profits for the producer. On the other hand, strategic patching does not aim at raising piracy costs as such. It instead focuses on curbing the cannibalization of the legal demand by piracy. Hence it is often the best choice when the overall demand is very high due to large positive network effects and the critical task facing the software producer is that of translating the strong overall demand to a strong demand for the legal version. This finding is important because it shows that software producers enjoying strong positive network effects for their products need not follow the practice of encouraging illegal channels. It also sheds light on Microsoft’s recent strategic switch to more restrictive patching practices.

However, my setting also has its own limitations. First of all, I have so far relied on numerical analysis. While such numerical analysis is mostly adequate for illustrating limitations of earlier research, it needs to be supplemented by analytical results. Also, I have omitted some important issues. For example, I have ignored the fact that many software products come in different versions [12], e.g., Professional, Home, etc. It would be an interesting exercise to find out whether my surprising findings regarding network effects remain applicable in situations where the same software product is offered in multiple versions. I intend to focus my future efforts on addressing some of these limitations.

References