TECHNOLOGY-FACILITATED

'GIVE ACCORDING TO YOUR ABILITIES, RECEIVE ACCORDING TO YOUR NEEDS'

Software, hardware, computer networks, and online content all require mechanisms to prevent free riding, overuse of common resources, use of resources without consent, and blocking of resource access.

Information technology, especially the Internet, facilitates the production, distribution, and consumption of products and services by increasingly following the principle of "Give according to your abilities, receive according to your needs," or GARN. Users contribute nonmonetary resources (such as programming skills, computing power, and network access) to a resource pool and draw similar resources from it. All this is done in return for no monetary reward, and giving or receiving can be at a level of zero; that is, users receive without giving or give without receiving. The GARN phenomenon is manifest in at least four contexts:

Software. Volunteer-based open-source software (OSS) initiatives (such as Linux) where code is created by volunteers and made available to the public;

Hardware. Organizational, interorganizational, and organizational/private grid computing initiatives (such as SETI@home, setiathome.berkeley.edu);

Networks. Wireless access points for wireless devices (primarily in urban areas); and

Content. Asset-based content contribution (such as P2P file-sharing systems) and knowledge-based content contribution (such as Wikipedia).

By Oded Nov and Bharat Rao

Like other nonexcludable goods, content lends itself to FREE RIDING.

Here, we compare these contexts using the GARN prism, identify the threats associated with the GARN phenomenon, and discuss ways to counter the threats. We provide a unified framework to phenomena that were previously viewed in isolation. Our aim is to unravel the common thread among Internet-facilitated contexts and consequently examine how lessons from one context may be used in others. Before exploring specific GARN phenomena, we turn to the economics literature and present several types of goods, as they are useful in our analysis.

		Nonrival	
		Low	High
Nonexcludable	High	Commons good	Public good
	Low	Private good	Collective good

Table 1. Types of goods [3].

Goods can be classified into four categories across the dimensions of nonexcludability and nonrivalry (see Table 1) [3]. For example, it is difficult to prevent nonexcludable goods (such as public parks) from being consumed by nonpayers; a nonrival (or nonconsumable) good (such as a TV show) can be consumed without diminishing its availability for future consumption. Unlike physical goods, information goods (such as software and content) are typically nonrival [11].

OSS development is a growing phenomenon [12], evident in the number of users registered at Sourceforge.net (a host for open-source projects, www.sourceforge.net) that increased from around 500,000 in 2003 [6] to more than 1.8 million in 2008. A growing variety of software applications are developed in the open-source model; more than 170,000 are registered at Sourceforge. Contributions are made by individuals independently deciding to donate time and effort to produce software that is freely available to all (a pure GARN) or by software companies actively supporting OSS development.

The availability of high-speed networks allows the sharing of computer resources via grid computing, enabling better allocation and use of computing resources within and among organizations. Grids may be closed (to members of a certain community) or open (accessible to all); they may also be one-way (contributors lack access to the pooled resource) or two-way (contributors are also receivers). A well-known example of a grid-computing project is SETI@home, a volunteer-based grid comparable to the strongest computer available today, for searching for "extraterrestrial intelligence." Computing grids can be viewed as grids of computers and primarily represent an architectural issue. However, our focus here is the wider issue of grids of computer users and owners, including their social and organizational implications.

Increasing use of wireless broadband computing is accompanied by the emergence of wireless commons, whereby participants provide Internet access to other participants through their WLAN access points [2]. Like computing grids, wireless commons may be either closed or open to all [2]. If the latter, which represents a pure GARN mechanism, individuals must not password-protect their access points.

Content GARN often manifests itself as contribution of content produced by others (such as media files shared via P2P systems). However, in many P2P networks, contributing and consuming are technically almost inseparable for users. Therefore, we won't analyze P2P networks here further. A clearer example of content GARN is knowledge-based, self-created content, such as Wikipedia, a free online encyclopedia with 1.4 million entries in English alone, written and edited by volunteers [7].

The GARN mechanism carries with it a number of threats that can be categorized using the goods typology (see Table 2); these are analyzed in the next sections. Given the common GARN mechanism

underlying the four contexts, each threat is followed by a discussion of the possible countermeasures, along with countermeasures used in other contexts that may be relevant.

Threat 1. Free riding, or asymmetry between giving and receiving. Asymmetry manifests itself as a lack of contributed resources for maintaining and improving the common pool of resources [2].

Contexts. OSS. OSS lends itself to free riding, as no contribution is requested in return for the use of freely available resources [12]. Countering the threat involves motivating potential contributors. This can be done by highlighting contributor benefits: learning from the expertise of peers in a technical community [6, 12]; being able to tailor software to one's personal needs [12]; having fun [9]; having the opportunity to signal status [5], potentially enhancing employment prospects [6, 10]; having the opportunity to support self identification [4]; and having the opportunity to help others.

Computing grids. In two-way grids, asymmetry of resource contributions can be countered through agreements among users to align receipt levels with contribution levels. In one-way grids, motivation to contribute is required in order to reduce free riding. The literature is limited on grid contribution motivations, but according to a SETI@home survey, the main one is "the good of humanity" (59% of respondents). Other motivations may include the performance of competing contributor groups. Motivations revealed in other contexts could also support contribution, including the public display of one's abilities, the prospect of self identification, and status signaling.

		Nonrival	
		Low	**High**
Nonexcludable	High	Wireless LAN -Commons good	OSS, wiki-based content -Public good
	Low	Private good	Computing grids -Collective good

Table 2. Typology of GARN-facilitated goods.

Wireless networks. Free riding manifests itself when a user password-protects his or her own access point or shuts it down when not using the commons [2]. Here, too, an effort to encourage the motivations discussed in the other contexts, including the prospect of self-identification and status signaling, helps reduce free riding.

Content. Like other nonexcludable goods, content lends itself to free riding. To mitigate against the limitations of online cooperation and collective action, online networks require ongoing interaction, identity persistence, and knowledge of previous interactions [5]. Other potential countermeasures discussed in the literature include: making people publicly commit to contribution; increasing social validity by demonstrating to potential contributors that many people like themselves have benefited from contributions; and creating contribution ratings by participants who rank contributors highly (the Slashdot model) [1]. In addition, countermeasures used in the OSS context may be useful, including incentives, such as the opportunity to display one's abilities and the opportunity to signal status and help others.

Threat 2. Use of others' resources without their knowledge or consent.

Contexts. OSS. Because OSS is nonexcludable, project hijacking is a potential threat, such as when an OSS is packaged with proprietary code in order to take it private [8]. Countermeasures include: adopting software that restricts proprietary appropriation; encouraging compliance with licensing terms through normative and legal sanctions; incorporation as a way to protect individual contributors from liability; transferring individual property rights to nonprofit corporations; trademarking a project's brands and logos; trademarking a foundation; and protecting a project's brand [8].

Computing grids. The threat is not significant in the grid context as long as contributing computers are protected from unauthorized access (excludability). Failure to provide this protection can result in others using their processing power or storage capacity. Ways to prevent the unwarranted use of resources includes: monitoring traffic; building firewalls; and establishing legal agreements among grid parties.

Wireless networks. Taking over contributors' devices is a significant threat; access is nonexcludable, making this commons good susceptible to the "tragedy of the commons." This threat can be countered through various security products [2]. In closed commons, it can be countered by monitoring the network for bandwidth use and removing devices that continuously overuse bandwidth [2].

Content. The threat here is the use of knowledge-based content produced without acknowledging the source. As both knowledge-based content and OSS are public goods, this threat can be countered in ways similar to the open-source software tactics identified in [8]. For example, Wikipedia is copyrighted, and proprietary appropriation is prohibited; Wikipedia is incorporated, and its contributors are protected from liability; individual property rights are transferred to a nonprofit foundation; and the Wikipedia brand is trademarked.

Threat 3. Overuse of resources. Also referred to as "overgrazing" in the literature [2] or free riding, it involves overuse without concern for the harm it causes others [10].

Contexts. OSS. The overuse of resources is not a significant threat to OSS; software, like many other information goods, is nonrival, and the cost of producing an additional unit of existing software is negligible.

Computing grids. In the case of two-way grids, the potential threat of overuse depends on agreements among the participants. In many cases, this threat is resolved by allowing a contribution only when the contributor computers are idle at the time of the contribution (so the resource becomes a nonrival good). In the case of one-way grids, the threat of overuse is mitigated against in a similar way, as resources are usually contributed only when the computer is idle.

	OSS	Computing grids (users)	WLAN	Content
Giving/ receiving asymmetry	Increase motivation - benefits for contributors: learning, become lead users, tailor software to needs, fun, signal status, signal ability, support self identification, help others	Increase motivation: public display of abilities, the prospect of self identification, and status signaling	Increase motivation: self identification, status signaling	Make people publicly commit to contribution, increase social validity, create contribution rating by other participants; increase motivation: display abilities, signal status, help others.
Use of others' resources without knowledge or consent	Adopt software that restricts such proprietary appropriation, encourage compliance with licensing terms through normative and legal sanctions, incorporate as a way to protect individual contributors, transfer property rights to nonprofit corporations; trademark brands and logos, trademark a foundation;, protect brand	Monitor traffic, firewall, establish legal agreements between parties involved in the grid	Use security products, monitor the network for bandwidth usage, and remove devices that overuse bandwidth	Prohibit proprietary appropriation, incorporate as a way to protect individual contributors, transfer property rights to nonprofit corporations trademark brands and logos, trademark a foundation; protect brand
Overuse of resources	Not relevant	Contribute only when resources are idle	Limit the number of receivers, limit access to the resource for a certain period	Not relevant
Preventing others from using resources	Not relevant	Oversight body to monitor and periodically analyze user complaints	Oversight body to monitor and analyze user complaints and removes offenders from the commons	Not relevant
Damaging a particular resource	Review before release	Not relevant	Vaccinate own devices, avoid use of hotspots with nonstandard equipment, quarantine infected devices, examine new access points	Use "change history" function to restore content. use alerts to monitor content changes, block user accounts, anonymous IP addresses, and IP ranges

Table 3. Threats and countermeasures.

Wireless networks. Here, the threat is significant, as wireless access is rival and nonexcludable; overuse of resources could result in their insufficient availability. Potential countermeasures include limiting the number of benefiting devices based on resource availability and limiting access to the resource for a certain period [2].

Content. In the case of knowledge contribution via Wikipedia and Wikipedia-like initiatives, the threat of overuse is low, as content, like software, is also a nonrival good.

Threat 4. Preventing others from using resources in order to increase one's own availability of resources.

Contexts. OSS. The threat of preventing others from using resources is not significant, as code is a nonrival good; preventing others' use of the resource provides little value.

Computing grids. The threat of being blocked from access is not significant in grids. However, a countermeasure would be like the one suggested in the case of wireless networks: having the oversight body monitor and periodically analyze user complaints.

Wireless networks. This threat manifests itself in the prevention of others' device operations so the remaining devices have more available bandwidth. It can be countered by assigning an oversight body to monitor and analyze user complaints, identify offenders, and remove the offender from the commons [2]. However, this method is possible only in closed commons where excludability is possible.

Content. As in OSS, this is not a major threat for content assets, as a content asset is a nonrival good.

Threat 5: Damaging resources.

Contexts OSS. Damage to resources is not a significant threat in the case of OSS, as software is reviewed and quality-controlled before it is released. Thus, the threat associated with nonexcludability is averted.

Computing grids. This is not a significant threat, due mainly to agreements among parties involved in computing grids and the ability to monitor members' behavior.

Wireless networks. As open commons are nonexcludable, this threat manifests itself in terms of someone adding a device with viruses to wireless commons or adding a device or access point that does not comply with 802.11X standards, possibly disrupting signals [2]. Ways to counter this threat in open commons include regularly vaccinating one's devices and avoiding the use of hotspots with nonstandard equipment. In closed commons, one should quaran-

The type of good largely determines the type and LEVEL OF VULNERABILITY to the threats associated with GARN.

tine infected devices and examine new access points for usability and standard compliance [2].

Content. Vandalism and corruption of files is relatively easy, as these are nonexcludable goods. A useful countermeasure against potential vandalism in Wikipedia is the "change history" function, which makes it easy to restore content. Moreover, the platform alerts users whenever a specific page is changed. In addition, potential vandalism stemming from differences over content may be thwarted by the fact that it is easy to create a new entry. In severe cases of vandalism, Wikipedia is able to block user accounts, anonymous IP addresses, and IP ranges (see Table 3).

CONCLUSION

The type of good largely determines the type and level of vulnerability to the threats associated with GARN. Volunteer-based OSS and knowledge-based content—both public goods—are susceptible to free riding, which in turn may be a major threat to their existence. However, being nonrival, software and content are not susceptible to threats stemming from nonexcludability. Computing grids are more easily protected from free riding due to their excludability and the agreements among participants in two-way grids. Motivational issues may help mitigate the associated threats. Wireless networks—another example of a common good—are susceptible to the threat of free riding.

The GARN phenomenon has implications for both business and policy making. One way for companies to take advantage of the GARN phenomenon is to operate as intermediaries between givers and receivers; for example, a company may create an exchange for such resources as content, network access, or computing power. Other potential ways to capitalize on GARN may be for companies to contribute resources and use this contribution as a vehicle for marketing (such as contributing network access and using it to display the company's logo and other messages).

In terms of policy making, GARN seems to offer a more efficient use of resources, allowing better access to products and services for people who otherwise could not afford it. At the same time, GARN involves legal implications (such as ownership of IP and responsibility for actions through GARN-available resources).

Further research is needed to better understand and utilize the GARN phenomenon. While we have applied a descriptive, qualitative focus here, it may focus on such issues as the motivational and behavioral factors underlying GARN, the economic analysis of this model, and its legal implications.

REFERENCES

1. Cheng, R. and Vassileva, J. User motivation and persuasion strategy for peer-to-peer communities. In *Proceedings of the Hawaii International Conference on System Sciences* 2005 (Mini-track on Online Communities in the Digital Economy/Emerging Technologies) (Hawaii, Jan. 3–6, 2005).
2. Damsgaard, J., Parikh, M., and Rao, B. Wireless commons: The tragedy and its causes. *Commun. ACM 49,* 2 (Feb. 2006), 105–109.
3. Frank, R. and Bernanke, B. *Principles of Economics.* Irwin/McGraw-Hill, New York, 2001.
4. Hertel, G., Niedner, S., and Herrmann, S. Motivation of software developers in open source projects: An Internet-based survey of contributors to the Linux kernel. *Research Policy 32* (2003), 1159–1177.
5. Kollock, P. Social dilemmas: The anatomy of cooperation. *Annual Review of Sociology 24* (1998), 183–214.
6. Lakhani, K., Spaeth, S., and von Krogh, G. Community, joining, and specialization in open source software innovation: A case study. *Research Policy 32* (2003), 1217–1241.
7. Nov, O. What motivates Wikipedians? *Commun. ACM 50,* 11 (Nov. 2007), 60–64.
8. O'Mahony, S. Guarding the commons: How community-managed software projects protect their work. *Research Policy 32* (2003), 1179–1198.
9. Osterloh, M., Rota, S., and Kuster, B. *Open Source Software Production: Climbing on the Shoulders of Giants. Working Paper,* 2003; opensource.mit.edu/papers/osterlohrotakuster.pdf.
10. Ostrom, E., Burger, J., Field, C., Norgaard, R., and Policansky, D. Revisiting the commons: Local lessons, global challenges. *Science 284* (1999), 278–282.
11. \Varian, H. Markets for information goods. In *Monetary Policy in a World of Knowledge-Based Growth, Quality Change, and Uncertain Measurement,* K. Okina and T. Inoue, Eds. Palgrave, New York, 2001.
12. von Hippel, E. and von Krogh, G. Open-source software and the private-collective innovation model: Issues for organization science. *Organization Science 14,* 2 (2003), 208–223.

ODED NOV (onov@poly.edu) is an assistant professor in the Department of Management, Polytechnic University, New York.
BHARAT RAO (brao@poly.edu) is an associate professor in the Department of Management, Polytechnic University, New York.

DOI: 10.1145/1342327.1342342