Panel IV

PROPERTIZING CYBERSECURITY

Nathan Alexander Sales
Syracuse University College of Law

Should the law grant intellectual property protection to cybersecurity information—in particular, information about system vulnerabilities, malicious code and other threats, and countermeasures against cyber intrusions? The tentative claim I plan to develop—with an emphasis on *tentative*—is that, while IP protections probably aren't necessary to create incentives to innovate, a carefully tailored IP regime for cybersecurity information would have a number of secondary benefits. It could facilitate market transactions that, through price signals, would help optimize levels of cybersecurity investment. Such a regime could foster a more robust market for cybersecurity insurance. And it could enable individuals and firms to specialize in producing different kinds of cybersecurity goods, perhaps resulting in efficiency gains.

This project, which I envision as a private-law companion to the public-law solutions I proposed in an earlier article entitled *Regulating Cybersecurity*, will begin by discussing the need to encourage cybersecurity innovation in the private sector. For reasons having to do with local knowledge and the costs of acquiring information, individuals and private firms will often know more than central regulators about vulnerabilities in the systems they use, the malware they face, and best practices for defeating intrusions.

Next, the project will consider the (relatively slight) legal protections available to various cybersecurity discoveries under existing IP law. Information about cybersecurity countermeasures may well be eligible for protection under patent law. But threat and vulnerability data probably is not propertizable—such information is little more than raw, unadorned facts, and cases like *Feist Publications v. Rural Telephone Service* and *Gottschalk v. Benson* hold that facts generally are neither copyrightable nor patentable.

The question then becomes whether the current lack of IP protection dissuades private firms and individuals from investing in cybersecurity research. Initially one might suspect the answer to be yes because of the potential free rider problems often associated with the production of information goods. In fact, however, even without IP protection private sector players devote considerable amounts of energy to generating information about cyber vulnerabilities, threats, and countermeasures. For instance, private companies like Kaspersky and McAfee do a brisk business selling security products to individual and corporate users. (These vertically integrated companies sell bundled goods that consist of software products capable of defeating various kinds of malware as well as access to the underlying databases of known malicious code on which the software relies.) In addition, recreational "white hat" hackers routinely hunt for vulnerabilities in commonly used software products, for reasons of simple intellectual curiosity or to burnish their reputations among their peers. Hence the primary justification for recognizing IP rights—incentivizing the creation of information goods—seemingly has little relevance here.

However, I expect to argue, recognizing some form of intellectual property in cybersecurity information could produce a number of secondary benefits that might independently justify such an IP regime. First, IP rights will facilitate market transactions in which cybersecurity information

is bought and sold. These transactions will send price signals that encode judgments about the relative severity of various vulnerabilities and threats and the likelihood they will produce harm. That in turn could help society adjust the resources it devotes to cybersecurity toward more efficient levels. Second, and relatedly, market transactions could result in a more robust market for cybersecurity insurance. Transaction data could make it easier for insurers and insureds to calculate the risk of intrusions, their likely severity, and the magnitude of the resulting damages—all of which are notoriously difficult to estimate. Third, IP rights could result more efficient ways of organizing production in the cybersecurity industry. At present, vertically integrated companies handle all aspects of product creation in house, from the discovery of threats and vulnerabilities to the creation of software. A new IP regime—with the ability to assign property rights via contract—might enable a division of labor in which firms specialize in different kinds of cybersecurity goods, with some focusing on threat detection and others on threat mitigation. The resulting efficiency gains might enable society to achieve greater levels of security at a lower cost.

The final section of the paper will discuss the specific contours of an IP regime for cybersecurity information. My initial thinking is that this would be a hybrid system drawing as needed from patent, copyright, and other fields of intellectual property. The rules would seek to maximize the benefits described above while at the same time minimizing the social costs that inevitably result when innovators are allowed to withdraw facts from the public domain and demand compensation when others use them.

So, for instance, we might follow copyright law and recognize an independent discovery doctrine. The risk that a researcher might be undercut by a subsequent rival would reduce the possibility of seller-side holdouts; it also would incentive innovators to sell their discoveries while they are still fresh and therefore at their highest social value. In addition, we might follow patent law and require innovators to register their discoveries with a central registry, thereby speeding the dissemination of data to those who would benefit from it. Finally, we might establish a broker akin to the performance right organizations seen in the copyright context. A cybersecurity broker could help reduce transaction costs—in particular, the seller's costs of locating an appropriate and willing buyer, and the buyer's costs of verifying the bona fides of the seller and the information on offer. A broker could also offset the imbalance of power between buyers (which tend to be powerful and sophisticated repeat players) and sellers (who often will be individual researchers seeking to sell a discovery for the first time), as well as mitigate information asymmetries (sellers of threat or vulnerability data will know considerably more about its quality than the buyers will).