Regulating Technical Design

Should software developers be required to include infringement-inhibiting components such as filters in their technologies?

Should technology developers be held legally responsible for misdeeds of their users if they design a technology that facilitates wrongful acts, such as copyright infringement? Should they have an obligation to build technologies to deter or inhibit wrongful acts? In the *Grokster* case, MGM argued that they should. The Supreme Court wasn't persuaded, ruling instead that technologists who actively induce users to infringe are responsible for those infringements (see the October 2005 "Legally Speaking" column).

Yet, the Court did not regard technical design as wholly irrelevant. When other evidence of inducement exists, technical design may be considered. The Court specifically mentioned failure to install filtering software in a peer-to-peer (P2P) file-sharing technology as a possible factor, although footnote 12 of the *MGM v. Grokster* decision says that failure to install filters is, by itself, insufficient for secondary liability.

No one knows how much evidence of inducement must exist before courts will start looking at technical design. But litigation threats have caused some P2P developers to start redesigning their systems. LimeWire has begun work to reconfigure its P2P technology to block the exchange of files for which it cannot verify authorization and eDonkey has announced its intent to install filters. Other P2P developers are reportedly considering this as well.

Before bowing to RIAA pressure to install filters, technologists should realize that courts in the U.S. have not imposed on them a duty to embed filters or other infringement-inhibiting features in general-purpose information technologies. Although MGM sprinkled its briefs with references to Grokster's failure to filter, there was no evidence before the Court about the feasibility or effectiveness of filtering technologies. There are many reasons to doubt whether filters will prevent copyright infringement to a meaningful degree. Courts should be very cautious in considering technical design, including decisions not to filter, as a factor in secondary liability cases.

LISA HANEY

The problems with filtering go beyond those discussed in the computer scientist brief.

Arguments for Filtering

Filtering came up in the *Grokster* case in several ways: MGM argued that Grokster was vicariously liable for user infringements because it could have designed its technology to inhibit user infringements by installing filters. An amicus curiae (friend of the court) brief submitted by several economists urged the Supreme Court to impose liability on technology developers if their failure to adopt alternative technical designs, such as filtering, enabled a large volume of infringement. Snocap and Audible Magic argued in amicus curiae briefs that they could provide filtering capabilities for P2P developers.

The main argument for filtering goes like this: Technologists are well positioned to design products to prevent or inhibit infringing uses. Developers of P2P technologies, in particular, have reason to know their products will be used for infringing purposes. By not trying to block infringements, technology developers impose huge costs on copyright owners. Making technologists build products that limit unauthorized copying would force them to internalize costs they are imposing on others (copyright owners).

The entertainment industry also believes technology firms should be responsible for user infringements because they make substantial profits from selling technologies that they have reason to know will be widely used to infringe copyrights. The market for information technology products is substantially larger because these products enable infringements. The more infringing uses or users there are for a technology, the larger will be its revenues. The entertainment industry considers much of the technology industry as "infringement-driven."

Computer Scientist Brief

Seventeen computer scientists—including Hal Abelson, Dan Boneh, David Clark, David Farber, Edward Felten, and Eugene Spafford—submitted an amicus brief to the Supreme Court in the *Grokster* case. The brief pointed out that the filtering technology for which MGM was arguing was as yet untested and unproven. Apart from self-interested assertions in the Snocap and Audible Magic briefs, there was no evidence that filters would be "effective in distinguishing infringing and noninfringing files if deployed in conjunction with software such as [Grokster's]."

MGM's suggested filtering strategy would, the brief noted, "require filtering software to be installed on users' computers." The brief questioned whether users would adopt updates of software with filters built in. Even after uploading filtering software, users might uninstall it. "End users ultimately have control over which software is on their computers."

The brief also raised concerns about the distorting effects a filtering obligation would have on the technical design decision making. "To order network designers to add functionality to the network to avoid liability is to force significant inefficiencies into network design." P2P technologies offer some important advantages for communications networks, such as enhanced robustness, which filters will undermine.

Omitting filters from one's technology "may represent good network design."

The brief predicted that a filtering obligation would "kick off an open-ended arms race between the filter designers and non-compliant users." Filters can be defeated. Napster made intensive efforts to develop filtering software to block exchanges of infringing files after the Ninth Circuit said it would be liable for infringements it didn't block. Users easily evaded file-name filters (for example, by typing N-i-r-v-a-n-a instead of Nirvana).

Napster also filtered for fingerprints and hashes, but they too were evaded by technically sophisticated users. Napster argued that it was doing its best to upgrade its filters to respond to evasions, but the trial judge overseeing the case ordered Napster to shut down unless it could filter at or near perfection (even though the Ninth Circuit had said perfection was not necessary). Notwithstanding concerted efforts of Napster's engineers and many highly skilled consultants, Napster was unable to consistently filter at this level. So it shut down.

Filtering technology has advanced since then. Today's filters focus on fingerprints (unique samples from audio files) or watermarks (hidden information to identify a file). Given the technical sophistication of so many users of digital information and the availability of digital networks to share information and electronic tools, it is foreseeable that watermark- and fingerprint-based filters will be defeated without undue difficulty. (Recall how easily that the watermarks promulgated by the Secure Digital Music Initiative (SDMI) were defeated several years ago by Ed Felten, his students, and colleagues when SDMI issued its "hacker challenge.")

Justice Breyer's concurring opinion in *Grokster* mentioned the computer scientist brief as casting doubt on filters as a workable solution to P2P file sharing. But Justice Souter and others on the Court seem to have taken MGM at its word that filtering is possible. If firms such as LimeWire and eDonkey adopt filters, judges may believe that filters have some utility in limiting infringement. To the arms race issue, judges may respond that efforts to defeat watermarks and fingerprints may violate the Digital Millennium Copyright Act (DMCA), and so can be regulated by this law.

Other Reasons to Question Filters

The problems with filtering go beyond those discussed in the computer scientist brief. Other problems include: when developers should consider filters and why; the interdependence of software components and implications of filters for redesigns; figuring out what to filter; where filters should reside in software; whether to allow unmarked files to be exchanged (as iMesh is doing with its "grey stars" program); what to do with legacy data; how to keep filters adequately up-to-date; whether a developer would have to extend the filters to all forms of copyrighted works; the global nature of the Internet and the local nature of any U.S. requirement for filtering; and questions about who should bear the costs of filtering.

Let's say you are developing a P2P technology for some legitimate purpose (for example, to enable faster downloads of open source software), but you know the technology is capable of infringing uses. You can take comfort in the Supreme Court's *Grokster* decision insofar as it recognizes advantages of P2P technology and states that you have no duty to install filters. But should you consider installing filters out of concern about misuses that might be made of your technology or fear that RIAA will sue you?

If you build in filters, it will cost a lot more to develop the technology and may make it perform less well. Insofar as filters overblock content (block files that lack authorization mark-up, but are non-infringing) or insofar as filters slow down the performance of your technology, you may worry that users will choose alternative technologies that perform better because they don't filter. Insofar as your filters underblock content (files with watermarks your filter didn't catch), you might worry that RIAA will still sue you. There may be little point in building filters if it means hav-

The task of building effective filters gets even more daunting when one considers that the Internet is a global communications network.

ing fewer customers or if doing so won't protect you against a lawsuit. How well must filters work before you be insulated from liability?

Now let's assume you developed a technology without filters and it's such a great technology that it has been widely adopted. Assume further that fans start using it to download a large volume of copyrighted movies or sound recordings. At this point, do you say to yourself "hey, I didn't induce any of this infringement and my technology has a substantial non-infringing use, so I've got nothing to worry about," or do you start thinking about how you could redesign your technology to install filters or whether you should strike a deal with a commercial filtering service?

To redesign your technology to install filters will be costly and time consuming. You've got many decisions to make, including what to filter for, whether to allow materials to pass through if they are unmarked (because they could be infringing copies), whether to use a commercial firm such as Snocap as a filtering service, how filters will work with other components of your technology, and how much redesign of other components will be necessary to accommodate the filters. It will not be simple to figure out how much such a redesign will cost, but let's assume you could do so.

Cost-Benefit Analysis

Can you also figure out how much copyright infringement your filters will avert and how much filtering would reduce entertainment industry losses? Judge Posner's cost-benefit test in *Aimster* calls for such a calculation. The comparative losses are to be weighed against the costs of installing infringement-inhibiting technologies such as filters. If the cost of installing infringement-inhibiting technology is not "disproportionately costly" as compared with infringement averted, *Aimster* says a technology developer that chooses not to adopt the inhibiting design should be secondarily liable for user infringements. (The Supreme Court did not endorse, but did not explicitly repudiate, the *Aimster* cost-benefit test.)

If you aren't confident your filters will be perfect (and how could they be?), you will soon discover that it is difficult to calculate the losses a filter would avert. Should you measure possible copyright damages by determining how much it would have cost users to buy swapped songs on iTunes or Rhapsody, by the average settlement amount per infringement obtained in lawsuits that RIAA has brought against individual file-sharers, or by copyright law's statutory damages rules?

Copyright law states that courts must award statutory damages if copyright owners want to receive them. Against non-willful infringers, courts can award damages anywhere between $750 and $30,000 *per infringed work*, as it deems just. Against willful infringers, courts can award damages up to $150,000 *per infringed work*.

If your technology is used by millions of people and billions of

files are exchanged through its use, measuring possible copyright "losses" in terms of statutory damages—what RIAA will argue for—will yield a very large number. Next to that number, the cost of redesigning your technology to install filters will almost certainly be small.

This means that insofar as courts follow Judge Posner's analysis in *Aimster*, you are likely to flunk the disproportionately costly test. If a judge decided that you should have installed filters, those same statutory damages will be sought against you. This just doesn't seem fair, especially if you make a good faith judgment that filters can't be effective.

Updates

Then there is the update issue. How can you possibly build a filter that will keep up to date with identifying information for all copyrighted works released in the future? RIAA firms may install watermarks into their existing inventory of sound recordings. Even if you could incorporate them into your filters, you would have a never-ending job to keep up with all the watermarks for works released in the future. (There is also a serious legacy issue with watermarks because of the enormous volume of copies of sound recordings that are not watermarked.) Much the same update problem would arise as to fingerprints.

Snocap wants to solve the update problem by providing filtering services for P2P and other developers. It has obtained identifying information for many digital recordings. There are, of course, some advantages if one firm is able to provide filtering technology for P2P developers. Snocap may aspire to become a proprietary standard in this market. But will one filtering company really be able to filter all files transmitted via P2P networks? Who will be responsible if copyrighted works aren't successfully filtered out? What if Snocap's servers crash? Wouldn't a single firm's technology be a magnet for hacker attacks to defeat it? Wouldn't such a firm also be in a position to charge monopoly rents and otherwise abuse monopoly power?

Attention thus far has mainly been focused on P2P sharing of sound recordings, but P2P technologies can be used to download motion pictures, software, and other digital works. Perhaps all commercial copyrighted works in digital form will need to be fingerprinted or watermarked. Technologists who build filters would find it very daunting, if not impossible, to filter for all copyrighted content on the Internet.

Global Internet

The task of building effective filters gets even more daunting when one considers that the Internet is a global communications network. The laws of some nations might require P2P developers to install filters, but other nations may not. This simple fact has consequences for whether local laws can be effective.

The only existing international consensus about secondary liability for copyright infringement is that liability should not be imposed merely because a firm provided the facilities used for infringement, whether those facilities are Internet access or P2P technology. Some nations have no secondary liability rules; some have more limited rules than the U.S. A Dutch court, for example, rejected a secondary liability claim against KaZaa for user infringement, although an Australian trial court recently held Sharman Networks, KaZaa's owner, liable for user copyright infringements, finding that under Australian law, KaZaa had a duty to filter for copyrighted materials. (That ruling is being appealed.)

Firms can respond to conflicting national rules by moving development to a jurisdiction where technologists are not responsible for user infringements. They would then be free to design innovative technologies without filters. They could still disseminate the technology throughout the world because software can be downloaded from a site where it is lawful. It can then be disseminated cheaply and rapidly via the Internet. (In a recent law review article, I gave this as an example of "intellectual property arbitrage.")

Even if you don't relocate, and even if you install filters, new versions of your technology minus the filters, or open source clones of your technology minus the filters, may still crop up and be disseminated via the Internet. For

example, eMule is a new open source version of the eDonkey technology. Moreover, as the lower courts realized in *Grokster*, users who already have P2P software on their hard drives can continue to use it to share files even if Grokster and other P2P developers are forced by litigation to shut down. The *Grokster* decision has not stopped or even slowed down P2P file sharing.

Conclusion

The Supreme Court rejected MGM's arguments for holding technology developers liable for designing infringement-enabling technology. Yet, it also said that technology design decisions, such as not using filters, may be considered if other evidence of inducement exists.

This column has shown that the Court was naïve in its belief about filtering as a workable solution to the P2P file-sharing phenomenon. If filtering cannot reasonably work, perhaps courts should give little weight to the Court's offhand and ill-informed statement about filtering.

Technologists must recognize that the entertainment industry wants courts to closely scrutinize many technical design decisions that arguably facilitate copyright infringement, including those that enable faster transmission of data, larger data storage capacity, anonymous file transfers, and playful uses of content that arguably allow creation of derivative works. (Clear Play was challenged as secondary infringer because its software enabled people to bypass sex, violence, and indecent language in DVD movies.)

The entertainment industry is determined to regulate infringement-enabling digital technologies. Its plans suffered one setback in *Grokster* and another when a federal appellate court struck down the FCC's "broadcast flag" rule on grounds that the FCC lacked jurisdiction from Congress to impose a requirement on makers of technologies capable of processing digital TV signals to conform to the "flag" (encoded information about permissible uses of the content). But this industry hasn't given up. Congress is already considering legislation to give the FCC jurisdiction to impose technical protection mandates for technologies capable of receiving or processing digital radio and television signals.

Grokster is thus only the first step in the next stage of the legal and policy debate about whether technical design should be regulated to protect the entertainment industry. It's too early to be complacent about the preservation of the *Sony* safe harbor for technologies with substantial non-infringing uses. The entertainment industry is still at war against it. C

Pamela Samuelson (pam@sims.berkeley.edu) is the Richard M. Sherman Professor of Law and Information Management at the University of California at Berkeley.