

Nanotechnology

WILL TINY PARTICLES CREATE LARGE LEGAL ISSUES?

BY ERNEST J. GETTO,
CYNTHIA H. CWIK,
AND L. DAVID RUSSELL

arious commentators contend that nanotechnology has the potential to spur the next Industrial Revolution. Still, many debate whether nanotechnology's impact will be beneficial or detrimental. Nanotechnology industry proponents bubble about the technology's potential. They assert that it may lead to "clean energy, zero-waste manufacturing and cheap space travel, if not immortality."¹ Nanotechnology's detractors match its proponents' conviction. They expect the worst, fearing that nanotechnology "will bring universal surveillance and harm the poor, the environment and human health—and may even destroy the whole planet through self-replicating 'grey goo.'"²

The public's view of these arguments merits close study. Eventually public opinion will determine, through legislation and the decisions of judges and juries, the legal response to nanotechnology. In response to changes brought by the Industrial Revolution, courts and legislators abolished the privity requirement, limited contributory negligence, invented strict liability and class action suits, and expanded government's regulatory powers. A nanotechnology revolution could lead to similarly large revisions of legal rules.

Even if nanotechnology's eventual impact is less than revolutionary, plaintiffs may still pursue suits against companies that utilize nanoparticles. Some commentators theorize that applications of nanotechnology may pose risks to human health and the environment. However, scientific evidence does not now, and may never, causally link nanoparticles with health or environmental problems. Nonetheless, plaintiffs may follow a recent litigation trend and pursue suits that disavow personal injury but still seek economic damages.

This article will explore nanotechnology's emerging trends and their potential legal implications. First, it will discuss the current and potential applications of the technology, acknowledging the opinions of both nanotechnology's proponents and detractors. Second, it will evaluate the public's reaction to nanotechnology. Third, it will briefly examine the limited judicial response to nanotechnology. Finally, it will analyze litigation issues that

may affect the field, drawing from asbestos litigation and more recent consumer class actions.

Applications of Nanotechnology

Nanotechnology generally refers to manipulating material on a nanometer scale. A nanometer is an extremely small unit of measurement equaling one billionth of a meter. Currently more than 800 products incorporating nanotechnology are produced by more than 400 companies located in more than 20 countries.³ These products accounted for more than \$88 billion in manufactured goods in 2007, and by 2016, it is estimated that goods incorporating nanotechnology will account for \$2.6 trillion in sales.⁴

Nanotechnology's small size makes it important. At the nanoscale level, particles have bigger surface areas and tend to be more reactive than larger particles, giving them novel properties. Nanotechnology has allowed manufacturers to make kitchen appliances bacterial resistant, sports equipment lighter and stronger, and clothes wrinkle free and stain resistant, to name just a few applications.

Eventually, scientists hope to use nanoparticles to directly treat diseases. Scientists are developing several types of these procedures, some of which have already demonstrated clinical success treating cancer. Scientists also believe that nanotechnology may one day be used to quickly and inexpensively remediate polluted soil and groundwater and purify drinking water. Finally, future applications of nanotechnology may lead to sustainable, "green manufacturing" techniques.

Ernest J. Getto is a partner in the litigation department of Latham & Watkins and practices in the San Francisco and Los Angeles offices. He has extensive experience in major litigation in massive environmental and toxic tort litigation. He can be reached at ernie.getto@lw.com. Cynthia H. Cwik is a partner with Latham & Watkins in San Diego. Her area of expertise includes complex civil litigation, including mass torts and class actions. She can be reached at cynthia.cwik@lw.com. L. David Russell is an associate in the San Diego office of Latham & Watkins. His area of expertise is litigation. He can be reached at david.russell@lw.com.

Whether nanoparticles pose danger to humans and the environment is currently unknown. Still, some allege that nanoparticles' unique characteristics may potentially cause harm. Nanoparticles' small size may allow them to enter the body through skin absorption, ingestion, inhalation, or direct injection for medical purposes. It has been argued that, once inside the body, nanoparticles' small size could allow them to enter the blood stream, cross membranes, invade cells, and transverse the blood brain barrier.⁵ Adding to theoretical concerns, a study recently determined that carbon nanotubes may have similar effects as asbestos on the lungs.⁶ However, this research is preliminary and has been strongly criticized.⁷

It has also been alleged that nanoparticles pose a danger to the environment, but again, little is known about the specific potential for harm. Still, nanotechnology's possible benefits, including its potential to help improve current environmental conditions, have even convinced some environmental groups to cautiously embrace the technology's "promising future."⁸

The Public's Reaction to Nanotechnology

A Divided Reaction

The American public's reaction to emerging nanotechnologies reflects the tension between the nanotechnology industry's proponents and detractors. On the one hand, "nano" is a marketing buzzword. For example, Apple's iPod Nano mp3 player (which, although not built on a nanoscale, does utilize nanotechnology) sold more than one million units in the 17 days after its release.⁹ The iPod Nano's popularity has been sustainable; Apple recently rolled out the fourth generation of the product.

On the other hand, many members of the American public remain skeptical and somewhat fearful of nanotechnology. Though case law related to this emerging technology is sparse, judges have written a handful of judicial opinions unrelated to patent litigation. In the majority of these opinions, pro se plaintiffs alleged that the government and other entities have harmed them by surreptitiously exposing them to nanoparticles. Not surprisingly,

the plaintiffs' allegations lacked proof, and most were quickly dismissed as frivolous.¹⁰ Potential plaintiffs, making similar complaints, have also visited online forums in attempts to recruit class action counsel to pursue their claims.¹¹ Although all the claims that have been filed to date almost certainly lack merit, it is worth noting that nanotechnology has become the focus of these litigants' anxiety.

In addition, consumer groups have aggressively petitioned the government and nanoparticle producers to increase regulation of nanotechnology. These groups advocate vastly different positions, from global moratoriums on nanotechnology research to requests for further governmental research and corporate disclosure of nanoparticle use. In response to this wave of "nanophobia," at least some companies that touted their use of nanoparticles have begun to distance themselves from the technology.¹²

Do You Believe in Magic (Nano)?

In March 2006, fears about nanotechnology seemed to be realized when a German bathroom cleaner called "Magic Nano" was recalled after it caused severe respiratory complications in more than 100 consumers. Magic Nano was purportedly made with silicon dioxide nanoparticles, which gave the product amazing cleaning properties. Most impressively, the manufacturer claimed that cleaning with Magic Nano would provide bathrooms with six months of antibacterial protection.¹³

Responding to the recall, the North American Action Group on Erosion, Technology and Concentration (ETC) called for a global nanotechnology research moratorium and complete recall of consumer products containing nanoparticles. However, consumers responded unexpectedly to this new health threat; in the midst of the health scare, the company that manufactured Magic Nano reported increased sales. The company claimed that, despite its association with a health scare, publicity of the product's impressive cleaning properties actually boosted the company's sales. In the end, any hysteria surrounding Magic Nano proved premature. Tests soon demonstrated that despite its name and manufacturer's claims, the cleaner contained no nanoparticles.

Nevertheless, ETC's position remained unchanged; a spokesman justified instituting the moratorium in order "to give . . . time to establish safety."¹⁴

The Public's Lack of Familiarity With Nanotechnology

The public's mixed reaction to nanotechnology can probably be explained by its lack of knowledge. A recent poll has found that half of American adults have never heard of nanotechnology, while only about seven percent "have heard a lot" about the technology.¹⁵ The public's perception of nanotechnology may very well be decisively influenced by the first well-publicized nanotechnology news story. As a result, at least one commentator has counseled nanotechnology companies to make sure the early products they market demonstrate "societal value."¹⁶ A recent study underscored the importance of the specific application of nanotechnology on public perception, finding that although the public may support utilizing advanced nanotechnology to improve human health, it may also disapprove of other advanced nanotechnology applications.¹⁷

Judicial Response So Far

As aforementioned, courts have yet to grapple with many nanotechnology-related lawsuits. However, when the issue of nanotechnology's potential harms has arisen, the judicial response has been restrained. In *Kennecott Greens Creek Mining Co. v. Mine Safety and Health Admin.*, 476 F.3d 946 (D.C. Cir. 2007), mining industry groups sought judicial review of three Mine Safety and Health Administration (MSHA) regulations. Petitioners argued that MSHA's rules limiting diesel particulate matter (DPM) emissions were flawed because they failed to acknowledge "that newer, cleaner engines—which are often necessary to reduce DPM exposure—may increase the number of dangerous 'nanoparticles' in mines."¹⁸

The D.C. Circuit disagreed with petitioners and deferred to the agency's expertise. The court acknowledged that MSHA's regulations may cause an increase in the production of nanoparticles and that these nanoparticles may be more harmful than DPM. However, the court reasoned that, because the risks of nanoparticles are

speculative while the risks of DPM are known, MSHA's scheme to regulate the known threat was not arbitrary and capricious.¹⁹ Until more is known about nanotechnology's potential risks, expect courts to continue responding conservatively to claims arising from nanotechnology.

Potential Litigation Issues

When any new technology is developed, lawsuits often follow closely behind. The plaintiffs' bar may begin pursuing nanotechnology-based claims in the coming years. Potential suits may follow one of two models. First, plaintiffs may pursue traditional personal injury tort suits. Alternatively, plaintiffs may pursue solely economic claims.

Traditional Personal Injury Suits: Asbestos Litigation as a Guide

Commentators, noting a study comparing similarities between carbon nanotubes' effect on the lungs to that of asbestos, have recently asked whether nanomaterials will spur "the next asbestos-like toxic tort . . ."²⁰ Although it is far from likely that nanotechnology will spur litigation on the same scale as asbestos litigation, plaintiffs may still pursue suits against nanoparticle manufacturers similar to the ones they pursued against asbestos manufacturers.

Earlier in the twentieth century, asbestos was lauded as a "magic mineral."²¹ Manufacturers took advantage of asbestos's resistance to heat and high tensile strength, increasingly incorporating it into many household products. Subsequently, some studies reported a relationship between some types of asbestos and certain health ailments.²²

Plaintiffs brought tort suits alleging direct injury from exposure to asbestos. Although the first few suits failed, in 1973 the Fifth Circuit unexpectedly extended strict liability to occupational diseases, allowing former insulator Clarence Borel to prevail.²³ Borel's success opened the door to an onslaught of suits. More than 8,400 companies have been named as defendants in more than 730,000 asbestos personal injury claims, paying a total of \$70 billion.²⁴

In these suits, plaintiffs often pursue duty to warn claims.²⁵ In most jurisdic-

tions, a manufacturer is required to warn only for dangers reasonably foreseeable at the time the manufacturer relinquishes control. Importantly, a manufacturer cannot be held liable for failing to warn about unknowable harms.²⁶ Thus, litigation often centers on the defendant's knowledge of asbestos's alleged dangers.

The overarching lesson the nanotechnology industry can learn from asbestos litigation is to take a cautious approach with an eye toward future litigation. Specifically, companies using nanoparticles should be wary of duty to warn suits and continuously evaluate their "knowledge" of nanotechnology's alleged harms. If they pursued a duty to warn theory, plaintiffs would likely argue that, based on the literature discussing nanoparticles' potential harmful effects, a company knew or should have known that its product would cause harm. In response, defendants would probably argue that, at the time of the exposure, they did not know and could not have known that their use of nanotechnology presented a health risk. To support this potential argument, companies should keep abreast of new studies regarding nanoparticles' health effects.

Economic Injury Suits: Recent Consumer Class Actions as a Guide

Recently, plaintiffs filed class actions in several different contexts claiming harm from products they alleged posed health risks. However, instead of pursuing traditional damages emanating from personal injury, plaintiffs often focused on recovering economic damages. Recent lawsuits concerning the amount of lead in lipstick illustrate this trend.

In October 2007, Campaign for Safe Cosmetics (CFS) published a study claiming that certain lipsticks contained dangerous amounts of lead. Although the FDA does not publish tolerance levels for lead in lipsticks, CFS based its assertion on FDA regulations limiting the amount of lead in candy. Because the amount of lead found in some lipsticks was purportedly higher than the FDA's limit for lead in candy, CFS concluded that these lipsticks may pose dangers to consumers.²⁷ Despite the obvious differences between candy consumption and lipstick consumption, plaintiffs soon filed suits against lipstick manufactur-

ers mimicking CFS's claims.²⁸

Plaintiffs argued that they would not have purchased the lipstick had they known of its lead content and pursued causes of action like breach of implied warranty, unjust enrichment, and statutory consumer fraud. They sought narrow economic damages, including the return of the purchase price and the costs of diagnostic testing and medical monitoring.²⁹ Although these individual claims seem small, once aggregated they still can represent significant liability.

Plaintiffs in these cases made additional personal injury allegations, contending that they had been injured by mere exposure to the lipstick and suffered an increased risk of being harmed by lead.³⁰ However, because they lacked actual injuries, a requirement for personal injury claims, courts sometimes dismissed these claims without discussion.³¹

The nanotechnology industry can learn from the "lead in lipstick" litigation. First, lawsuits and legislation can quickly spring up across the country after the publication

of a nonconclusive, but headline-catching, study. Manufacturers utilizing nanotechnology should prepare for a similar reaction if studies drawing negative attention to nanotechnology are released, regardless of their conclusiveness. Second, if plaintiffs file nanotechnology-related suits, they may decide to pursue consumer class actions instead of personal injury claims. Based on the existing body of scientific knowledge, it would be extremely difficult for plaintiffs pursuing nanotechnology claims to prove causation.³²

Preparing for the Unknown

Nanotechnology has the potential to positively impact the world in revolutionary ways. Technologies utilizing nanotechnology may one day cure disease, efficiently remediate pollution, and provide clean energy sources, among other applications. Still, while its potential is intriguing, the harms nanotechnology presents, if any, are currently unknown. Additionally, a large majority of the public lacks knowledge of nanotechnology's very existence; it

remains to be seen whether this silent majority will embrace nanotechnology.

Although product liability law is inherently unpredictable, these factors may magnify the law's fickleness, making the outcomes of nanotechnology-related lawsuits even more difficult to predict. Therefore, to minimize potential liability, companies utilizing nanotechnology have a difficult task; they must prepare for the unknown. This task necessarily requires taking a cautious approach. When possible, companies utilizing nanoparticles should try to protect consumers and workers from potential risks, including considering disclosures, warnings, and protective equipment for workers in appropriate circumstances. This responsible approach will not only provide protection from liability but will also help garner public support for companies that utilize nanotechnology. ♦

Endnotes

1. *Small Wonders*, *ECONOMIST*, Jan. 1, 2005.
2. *Id.*; see also K. ERIC DREXLER, *ENGINES*

continued on page 15

SHIFTING STRATEGIES FOR PROTECTING MUSIC ONLINE

DMCA Takedown Notices, Litigation, and Cooperative Approaches

By William Sloan Coats
and
Julieta L. Lerner

Even though it has been almost a decade since an injunction issued against Napster,¹ the music industry has continued to grapple with how to stop users from sharing music files and (more commonly now) video clips containing music on the Internet. One strategy available to copyright holders is to issue takedown notices to Internet service providers (ISPs) under the Digital Millennium Copyright Act (DMCA), which requires ISPs, in accordance with the procedures set forth, to take down allegedly infringing material. As long as ISPs comply with the procedures, they benefit from the safe harbor provisions that insulate them broadly from liability for infringement. Until recently, content owners essentially only needed to consider whether the posting of their content violated their rights, but this analysis may have become more complex. In May of 2008, the court in *Lenz v. Universal Music* held that content owners have a responsibility to consider the Fair Use Doctrine in determining whether to issue a takedown notice. An-

other strategy copyright holders rely on involves bringing lawsuits against technology companies and, more controversially, against individuals. After years of focusing on litigation, which has often attracted negative publicity, the record labels are shifting towards a "graduated approach." In December 2008, the Recording Industry Association of America (RIAA) announced a policy under which, rather than resorting to litigation, it will work with ISPs to provide notice and gradually increasing sanctions against users infringing on their rights.

Protections and Responsibilities Under the DMCA

The DMCA was signed into law in 1998.² Among its many provisions, the DMCA provides a mechanism by which content owners can notify ISPs of infringing content and by which the ISPs must take down this content. In exchange for compliance, the law shelters ISPs from claims of copyright infringement made against them that result from the conduct of their customers.

Content Owners

For the ISP to remove allegedly infringing materials from its network, the content owner must provide, in addition to information identifying itself and the allegedly infringing materials, a statement that the owner had a "good faith belief" that there is no legal basis for use of the materials at issue.³ When it comes to the sharing of music, usually the content owner's rights stem from section 106(1) of the Copyright Act, which grants the exclusive right to reproduce the copyrighted work in copies and section 106(3), which grants the exclusive right to distribute copies to the public; the right of public performance, in section 106(4), may also be involved.⁴

The DMCA does not require content owners to notify the individuals responsible for the allegedly infringing material. However, the safe harbor provisions require ISPs to notify subscribers if their materials have been removed and to provide them with an opportunity to send a written notice



son dancing in her kitchen, while Prince's "Let's Go Crazy" played faintly in the background. Universal, which owns the copyright to "Let's Go Crazy," sent YouTube a DMCA takedown notice, demanding that YouTube remove the video for violating Universal's copyright. YouTube removed the video the following day and sent Lenz an email notifying her it had removed the content and warning her that repeated incidents of copyright infringement could lead to the deletion of her account and all of her videos. Lenz responded with a counternotice, demanding that the video be reposted, and YouTube reposted the video about six weeks later.⁷

In an unusual turn of events, Lenz filed suit against Universal on July 24, 2007. Universal then successfully moved to dismiss the claims of Lenz's original complaint. The court permitted Lenz to replead the complaint, which Lenz did. On May 23, 2008, Universal filed a motion seeking to dismiss Lenz's only claim, a claim for misrepresentation under 17 U.S.C. section 512(f).⁸ Neither party disputed that Lenz used copyrighted material in the video. Despite this, Lenz argued that the DMCA requires the copyright owner to consider the Fair Use Doctrine in formulating a "good faith belief" under 17 U.S.C. section 512(c)(3)(A)(v) that "use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law."⁹ Universal countered that because fair use is an excused infringement, copyright owners cannot be required to evaluate the question of fair use prior to sending a takedown notice.¹⁰ The court found that copyright holders are required to engage in a good faith consideration of whether a particular use is fair use.¹¹ Further, the court found that an allegation that a copyright owner acted in bad faith in issuing a takedown notice without proper consideration of the Fair Use Doctrine is sufficient to state a claim for misrepresentation under section 512(f) of the DMCA.¹²

to the ISP stating that the material has been wrongly removed. If a subscriber provides a proper "counternotice" claiming that the material does not infringe copyrights, the ISP must then promptly notify the claiming party of the individual's objection, and, unless the copyright owner brings lawsuit in district court within 14 days, restore the material to its network.⁵

Under a recent holding, the copyright holder has a responsibility to consider the Fair Use Doctrine in determining whether to issue a takedown notice. In a case that drew wide media attention, likely due to a particularly sympathetic plaintiff, an individual by the name of Stephanie Lenz sued Universal Music Corporation (Universal, a record label) regarding a takedown notice that Universal had issued and voluntarily retracted.⁶ Lenz had placed on YouTube.com a 29-second video of her 13-month-old

William Sloan Coats is a partner and Julieta L. Lerner an associate at the Palo Alto office of White & Case LLP.

ISP Safe Harbor

Courts have interpreted the DMCA as providing broad protection to ISPs. The DMCA provides that an online entity shall not be liable for storing infringing material at the direction of a user if the entity qualifies as an ISP and if the ISP can satisfy a number of conditions concerning knowledge, financial benefit, and notification. For purposes of the DMCA's safe harbor, an ISP is defined as "a provider of online services or network access, or the operator of facilities therefore."¹³ The definition of ISP is "broad."¹⁴ The online auction and shopping sites, eBay.com and Amazon.com, and the file sharing service, Aimster, all qualified as ISPs.¹⁵

To be eligible for the limitations on liability provided by the DMCA, the ISP must have adopted and reasonably implemented "a policy that provides for the termination in appropriate circumstances of subscribers and account holders . . . who are repeat infringers."¹⁶ The ISP must inform subscribers and account holders of this policy.¹⁷ Also, the ISP must accommodate and not interfere with standard technical measures used by copyright owners to identify and protect copyrighted works.¹⁸

What qualifies as a "reasonable implementation" of a repeat infringer termination policy has been the subject of litigation. In *Ellison v. Robertson*, the Ninth Circuit determined that there was an issue concerning whether America Online (AOL) had reasonably implemented its policy as required by section 512(i) when AOL had changed the address to which notifications were sent but did not forward messages from the old address or notify subscribers of the change.¹⁹ Similarly, the Seventh Circuit found that Aimster failed to implement a repeat infringer policy reasonably, where its encryption method made it impossible for the ISP to determine which files were being transferred by which user and hence who was responsible for copyright infringement.²⁰

An ISP eligible for the limitations

on liability will not be liable for music or other content that infringes copyright so long as the ISP "does not have actual knowledge that the material . . . on the system or network is infringing," or is not "aware of facts or circumstances from which infringing activity is apparent," or "upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material."²¹ Additionally, the ISP must not "receive a financial benefit directly attributable to the infringing activity" in a situation where "the service provider has the right and ability to control such activity."²² Upon notification of claimed infringement, the ISP must respond expeditiously to remove or to disable access to the infringing material. The ISP must designate an agent to receive notifications of claimed infringement and provide information concerning the designated agent to the Copyright Office.²³

Copyright Enforcement Through Litigation

When the DMCA takedown procedures or other measures fail to offer a copyright holder sufficient recourse, the copyright holder may resort to litigation. Copyright holders were somewhat successful in curbing some of the more egregious cases of copyright infringement involving the sharing of music online by targeting the companies responsible for the file sharing technology. The record labels have also targeted individual users for sharing files. The labels have sued thousands of individuals,²⁴ resulting in much negative publicity and questioning of the effectiveness of these methods.²⁵

Although many of the legal issues involving these cases have been resolved, a debate remains among the circuits whether making music available online violates the exclusive right of reproduction and distribution under the Copyright Act. Although most courts require that the plaintiff show that defendant has actually distributed a copy to a member of the public, some courts have found that merely making a copy available is sufficient for liability.²⁶

Cooperative Enforcement Strategies

The RIAA is ending its "broad-based end user litigation program,"²⁷ an approach that often led it to be painted as a villain in the media.²⁸ In December 2008, the RIAA announced plans to shift from bringing lawsuits against individual users in favor of a "graduated response" partnership with ISPs.²⁹ The step was part of what the RIAA described as "a real movement toward ISPs assuming a more proactive role in dealing with online piracy in a constructive way that's sensitive to their subscribers." Under the plan, the RIAA will identify an act of infringement and alert the ISP that one of its customers is allegedly sharing files, and the ISP will notify its customer. The RIAA will use technology that it believes can reliably identify illegal file sharing and avoid "false positives."³⁰ If the customer does not reply to repeated notices that it may be sharing files in violation of another's copyright, the ISP may terminate service to the customer.³¹

In many ways, this program appears similar to measures already in place under the DMCA, which require ISPs to have a repeat infringement termination policy to qualify for safe harbor protection. The key difference appears to be greater coordination between the RIAA and ISPs, paired with the RIAA's commitment to avoiding lawsuits against individuals. By shifting its strategy, the RIAA may meet its goal of working together with ISPs in a way that will improve public perceptions, while increasing the recording industry's ability to protect its content. ♦

Endnotes

1. *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (N.D. Cal. 2000) (granting a preliminary injunction enjoining Napster from "facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs' copyrighted musical compositions and sound recordings"); *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001) (remanding for modification of the protective order, because the injunction was overbroad in that it placed the entire burden of policing infringement of plaintiffs' works on Napster).

2. U.S. Copyright Office Summary, *The Digital Millennium Copyright Act of 1998*

(Dec. 1998), www.copyright.gov/legislation/dmca.pdf.

3. Digital Millennium Copyright Act, 17 U.S.C. § 512(c)(3)(A)(i-vi).

4. Copyright Act, 17 U.S.C. § 106.

5. DMCA § 512(g)(2).

6. *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150, 1151-52 (N.D. Cal. 2008). On Oct. 28, 2008, the court denied Universal's motion to certify the order for interlocutory appeal. *Lenz v. Universal*, 2008 WL 4790669 (N.D. Cal.).

7. *Lenz*, 572 F. Supp. 2d at 1151-52.

8. *Id.* at 1153.

9. *Id.* at 1153-54.

10. *Id.* at 1154.

11. *Id.* at 1156.

12. *Id.* at 1156-57.

13. DMCA § 512(k)(1)(B).

14. *In re Aimster Copyright Litig.*, 334 F.3d 643, 655 (7th Cir. 2003).

15. *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1100 (W.D. Wash. 2004); *In re Aimster Copyright Litig.*, 334 F.3d at 655 ("[T]he definition of Internet service provider [contained in § 512(k)(1)(B)] is broad" and "Aimster fits it").

16. DMCA § 512(i)(1)(A).

17. DMCA § 512(i)(1)(A). For example, YouTube has a policy under which it will terminate a user's access to its services if the user is "determined to be a repeat infringer." YouTube, Terms of Service, www.youtube.com/t/terms.

18. DMCA §§ 512(i)(1)(B) and 512(i)(2).

19. 357 F.3d 1072, 1080 (9th Cir. 2004).

20. *In re Aimster Copyright Litig.*, 252 F. Supp. 2d at 659.

21. DMCA § 512(c)(1)(A).

22. DMCA § 512(c)(1)(B).

23. DMCA § 512(c)(2).

24. Sarah McBride and Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 29, 2008, <http://online.wsj.com/article/SB122966038836021137.html> (claiming the record labels have brought suit against 35,000 individuals since 2003).

25. See, e.g., Antone Gonsalves, *RIAA Taps ISPs to Fight Illegal Downloads*, INFORMATION WEEK, Dec. 19, 2008, www.informationweek.com/news/personal_tech/music/showArticle.jhtml?articleID=212501507&subSection=Management.

26. See *London-Sire Records, Inc. v. Doe*, 542 F. Supp. 2d 153, 176 (D. Mass. 2008) ("[M]erely exposing music files to the inter-

net is not copyright infringement."); Atlantic Recording Corp. et al. v. Howell, 554 F. Supp. 2d 976, 981 (D. Ariz. 2008) (The "great weight of authority" establishes that section 106(3) "is not violated unless the defendant has actually distributed an unauthorized copy of the work to a member of the public."); but see Maverick Recording Co. v. Harper, 07-CV-00026, Order (W.D. Tex. Aug. 7, 2008) ("The fact that the Recordings were available for download is sufficient to violate Plaintiff's exclusive rights of reproduction and distribution. It is not necessary

to prove that all of the Recordings were actually downloaded.").

27. RIAA, For Students Doing Reports, www.riaa.com/faq.php.

28. See, e.g., Iain Thomson and Shan Nichols, *Top 10 IT Villains*, VNUNET, Mar. 28, 2009, <http://uk.news.yahoo.com/16/20090328/ttc-top-10-it-villains-6315470.html> (choosing RIAA as the number one villain, explaining the "RIAA's campaign of suing those who did nothing more than download a single song on a P2P network was reckless at best and epically

malicious and arrogant at worst").

29. Greg Sandoval, *RIAA Drops Lawsuit; ISPs to Battle File Sharing*, CNET News, Dec. 19, 2008, http://news.cnet.com/8301-1023_3-10126914-93.html?tag=mncol;txt.

30. Nate Anderson, *RIAA Graduated Response Plan: Q&A with Cary Sherman*, ARS TECHNICA, Dec. 21, 2008, <http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars>.

31. Sandoval, *supra* note 29, and Anderson, *supra* note 30.

Nanotech Legal Issues

(continued from page 9)

OF CREATION THE COMING ERA OF NANOTECHNOLOGY (Anchor Books 1986), available at www.e-drexler.com/d/06/00/EOC/EOC_Cover.html.

3. PROJECT ON EMERGING NANOTECHNOLOGIES, CONSUMER PRODUCTS INVENTORY, www.nanotechproject.org/inventories/consumer/ (last visited Dec. 30, 2008).

4. *The Next Big Thing in Nanotechnology? Litigation*, NANOWERK NEWS, Aug. 18, 2008, www.nanowerk.com/news/newsid=6792.php.

5. U.S. ENV'TL. PROT. AGENCY, EPA 100/B-07/001 NANOTECHNOLOGY WHITE PAPER 13-14 (2007); LLOYD'S OF LONDON, NANOTECHNOLOGY RECENT DEVELOPMENTS, RISKS, AND OPPORTUNITIES 13-14 (2007), <http://www.lloyds.com/NP/rdonlyres/7C1D8222-A3E8-4781-8C80-http://www.epa.gov/OSA/pdfs/nanotech/epa-nanotechnology-whitepaper-0207.pdf> [hereinafter EPA White Paper].

6. C. Poland et al., *Carbon Nanotubes Introduced Into the Abdominal Cavity of Mice Show Asbestos-Like Pathology in a Pilot Study*, NATURE NANOTECH., May 20, 2008.

7. See John C. Monica, Jr. & John C. Monica, *A Nano-Mesothelioma False Alarm*, 5 NANOTECHNOLOGY L. & BUS. 319 (2008).

8. *Nanotechnology's Double-Edged Sword*, Environmental Defense Fund, Sept. 26, 2007, www.edf.org/article.cfm?contentID=4449.

9. Daniel D. Turner, *Apple Hits \$1 Billion in Profit for 2005*, eWeek.com, Oct. 11, 2005, www.eweek.com/c/a/Apple/Apple-Hits-1-Billion-in-Profit-for-2005/.

10. See *Lewis v. Univ. Med. Ctr.*, No. 4:07cv3012, 2007 WL 2123753 (D. Neb. Jul. 20, 2007); *Roun v. Bush*, 461 F. Supp. 2d 40 (D. D.C. 2006); *Jackson v. Roun*, No. W2000-02974-COA-R3-CV.2001 WL 1516996.

(Tenn. Ct. App. Nov. 26, 2001).

11. Posting of iceni6 to <http://sueasy.com>, Aug. 26, 2008 (last visited Nov. 4, 2008).

12. Natasha Singer, *New Products Bring Side Effect: Nanophobia*, N.Y. TIMES, Dec. 3, 2008.

13. David Graber & Pat Phibbs, *German Institute Working to Understand Why "Magic Nano" Cleaner Caused Ailments*, 34 PROD. SAFETY AND LAB. REP. 390 (2006); Andreas von Bubnoff, *Study Shows No Nano in Magic Nano, the German Product Recalled for Causing Breathing Problems*, SMALL TIMES, May 26, 2006, www.smalltimes.com/Articles/Article_Display.cfm?ARTICLE_ID=270664&cp=109, *Has All The Magic Gone?* ECONOMIST, Apr. 15, 2006.

14. von Bubnoff, *supra* note 13; *Has All The Magic Gone?*, *supra* note 13.

15. Peter D. Hart Research Associates, Inc., *Awareness of and Attitudes Toward Nanotechnology and Synthetic Biology: A Report of Findings Based on a National Survey Among Adults* (2008), www.nanotechproject.org/process/assets/files/7040/final-synbioreport.pdf.

16. *Much Ado About Almost Nothing*, ECONOMIST, Mar. 20, 2004.

17. *Survey Highlights Support for Nanotech in Health Fields But Disapproval Elsewhere*, Biomedicine.org, Nov. 13, 2008, www.biomedicine.org/biology-news-1/Survey-highlights-support-for-nanotech-in-health-fields-but-disapproval-elsewhere-5850-1/.

18. *Kennecott Greens Creek Mining Co. v. Mine Safety and Health Admin.*, 476 F.3d 94, 954 (D.C. Cir. 2007).

19. *Id.*

20. Rob Bac, *Nanomaterials: The Next Asbestos-Like Toxic Tort or the Greatest Thing Since Sliced Bread*, <http://law.lexisnexis.com/practiceareas/Emerging-Issues-Law-Blog/Emerging-Issues/>

Nanomaterials—the next asbestos-like toxic tort or the greatest thing since sliced bread (last visited Dec. 30, 2008).

21. Edward J. McCambridge, *Asbestos Litigation: Where We Have Been, Where We Are Now, Where We Are Going*, 57 FED'N DEF. & CORP. COUNS. Q. 409, 423 (2007).

22. See *Threadgill v. Armstrong World Indus., Inc.*, 928 F.2d 1366 (3d Cir. 1991).

23. *Borel v. Fibreboard Paper Prod. Corp.*, 493 F.2d 1076, 1106 (5th Cir. 1973).

24. Susan Cornwell, *Asbestos Costs US Companies \$70 Billion So Far*, REUTERS NEWS, Feb. 6, 2004.

25. MARGIE SPARCY-ALFORD, *A GUIDE TO TOXIC TORTS*, §21.02 (2008).

26. JOHN F. VARGO et al., *PRODUCTS LIABILITY PRACTICE GUIDE*, §§6.03, 7.03 (John F. Vargo ed. 2008).

27. The Campaign for Safe Cosmetics, *A Poison Kiss: The Problem of Lead in Lipstick* (Oct. 2007), available at http://safecosmetics.live.radicaldesigns.org/downloads/A%20Poison%20Kiss_report.pdf; U.S. Food & Drug Admin., *Lipstick and Lead: Questions and Answers* (Dec. 27, 2007), www.cfsan.fda.gov/~dms/cos-ph.html.

28. See *Frye v. L'Oreal USA Inc.*, 583 F. Supp. 2d 954 (N.D. Ill. 2008); *Koronthaly v. L'Oreal USA, Inc.*, No. 07-CV-5588 (DMC), 2008 U.S. Dist. LEXIS 59024 (D.N.J. Jul. 29, 2008), *motion for recons. den.* 2008 U.S. Dist. LEXIS 86419 (D.N.J. Oct. 24, 2008).

29. *Frye*, 583 F. Supp. 2d at 956-58; *Koronthaly*, 2008 U.S. Dist. LEXIS 59024 at *4-5; *Koronthaly*, 2008 U.S. Dist. LEXIS 86419 at *3.

30. *Koronthaly*, 2008 U.S. Dist. LEXIS 86419 at *3.

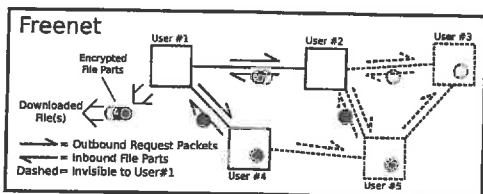
31. *Frye*, 583 F. Supp. 2d at 959.

32. See *Monica*, *supra* note 7, at 331-32.

Anonymity Networks: Hiding in Plain Sight

By Richard Abbott

There are places on the Internet that are hidden. They are places to meet and trade information without worry of censorship or law enforcement. There are no secret handshakes, rituals, or dues to pay. Structures called *anonymity networks* provide access to and protect these places from outside observation. Paradoxically, while nobody can find these places physically, anyone can access them. In this very brief article I will describe three of these anonymity networks, but there are many more out there. Structurally, each is unique, but they are all free, open-source projects maintained and administered by members of the public. They all hide activities and websites that cannot be tracked, cannot be turned off, and laugh in the face of the Digital Millennium Copyright Act (DMCA), Communications Assistance for Law Enforcement (CALEA), and most every other legal restriction.



Freenet

<http://freenetproject.org>

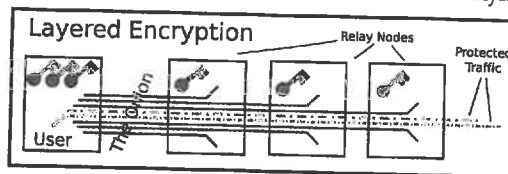
Freenet is the aging grandfather of anonymity networks. In essence, Freenet is a complex file sharing scheme. All users accessing the network agree to allow their computers to act as relay nodes. Each donates a combination of drive space and bandwidth for the use of the network. Those wanting to share files first encrypt them, break them into parts, and scatter the parts among nearby nodes. Hidden

Richard Abbott is an Oregon attorney and IT privacy consultant. Specializing in countersurveillance, Richard works with businesses and individuals trying to safeguard data from threats ranging from wiretaps to hardware theft. Richard is also a staunch supporter of Free/Open Source Software (F/OSS). He can be reached at Rabbit@shaw.ca or OregonRabbit@hushmail.com.

websites, called *Frebsites*, are published by sharing their html files. Downloading is accomplished by handing request packets from node to node. When a request finds the wanted file piece, that piece is sent back down the path left by the outbound request. This means nobody can tell where a request came from, or where a file part is going. Nodes take notice of the file parts they handle most often. Copies of popular files parts are retained and stored locally. Heavily requested files therefore propagate throughout the network, while unpopular files become rare and eventually disappear. Freenet's greatest strength is the survivability of the collective data store. Removal of any one machine eliminates nothing from the collective network. This means a file or freesite will remain online long after its publisher has left the network. A very popular file could prove impossible to ever remove.

Layered Encryption

The next two networks rely on layered encryption schemes. By wrapping traffic within layers of encryption, these networks allow users to build and administer pathways through multiple proxies without worry of either outside wiretappers or turncoats within the network. Both TOR and I2p use versions of this scheme.

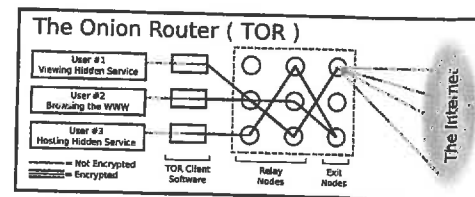


The Onion Router (TOR)

www.torproject.org

TOR is currently the most established anonymity network. Created by the U.S. Navy and released to the public in 2004, TOR is designed to allow users to anonymize otherwise normal Internet connections. TOR relies on those users who are willing to host encrypted relay nodes. Such TOR nodes can be hosted on any computer connected to the Internet. There are normally more than a thousand active nodes, but anyone may access the

network whether they want to contribute or not. By routing traffic via *circuits* of at least three nodes, users access the Internet without exposing their IP addresses. Similarly, users can link a web server to a TOR circuit and play host to a *hidden service*. This creates untraceable websites accessible only to those connected to TOR.

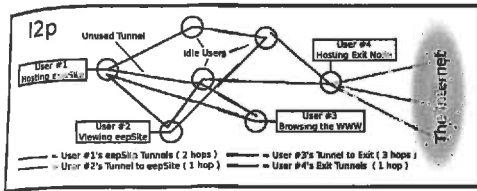


TOR is also used to bypass censorship. By routing their connection through TOR, users escape from under censorship regimes such as China's *Great Firewall* (or *Golden Shield*, depending on your perspective). Similarly, because TOR allows users to route their connections through foreign exit nodes, anyone can test how websites react to users from different countries. Want to see how Google.fr lists your website? TOR allows you to adopt a French IP address and see for yourself: no costly IT consultant needed.

I2p

www.i2p2.de

I2p is the latest and most-evolved anonymity network. I2p employs TOR-like circuits called *tunnels*, the length of which can vary to accommodate different security needs. All users must operate a node and contribute bandwidth, but unlike Freenet, I2p users are not obligated to play host to any material. Instead, users voluntarily share files via their individual connections. Shorter connection paths, fewer and more polite connections between nodes, and the ability to handle both TCP and UDP packets all add up to much greater and more stable speeds. I2p is currently the only anonymity network able to sustain swarm downloading, but this occurs entirely within the network. Websites hidden within i2p are called *eepSites* and are essentially the same as TOR's hidden services.



At time of writing, there was one operational exit node allowing those within I2p to anonymously browse the normal Internet. Access to the normal Internet is not now, and never will be, part of I2p's overall design. The one operational node is solely a product of its host.

Consequences for Copyright Enforcement Efforts

Internet protocol addresses mean nothing when dealing with file transfers passing through anonymity networks. Any IP address detected on the normal Internet will in fact be that of an exit node, not the actual wrongdoer. DMCA takedown notices sent to exit node operators are misplaced, as no material actually resides at the exit node. Similarly, any subpoena, DMCA or otherwise, will not yield the identity of the wrongdoer. Exit nodes handle general Internet traffic. Any recording of user-identifiable information would therefore constitute illegal wiretapping. Even if such records existed, they would only ever point to other nodes deeper within the network. These networks work under the assumption that many governments are actively trying to break them. They incorporate the possibility of enemy-controlled nodes into their threat models. Record keeping, even mandated record keeping, is not the answer.

This article proposes that there are solutions, but they require a mature approach. The addiction to IP addresses must be broken. The practice of blindly firing off takedown notices without regard should stop. Copyright holders must instead check any detected IP address against the published lists of exit nodes. They then need to cooperate with exit node operators. Most exit node operators actually want to eliminate file sharing via their nodes because it takes bandwidth from more noble causes. These operators can block access to IP addresses belonging to hosting services and can work to

cut off peer-to-peer networks by blocking the associated ports and protocols. These strategies require effort, but they do work and are the only legal and effective avenues for addressing such problems.

File sharing that remains wholly within anonymity networks is another matter. Such communication is beyond any legal enforcement efforts. This does not mean that copyright is dead. Copyright holders should remind themselves of just how slow these anonymity networks currently are. Even within I2p, large movie files take hours or days to download. Nobody is sharing Blu-ray movies just yet. Mp3s are certainly at risk, but frankly those are freely traded via the normal Internet already. That may change if groups like the Recording Industry Association of America (RIAA) start actually making headway. Anonymous file sharing is out there, just waiting for users to make the switch.

Consequences for Law Enforcement

These anonymity networks contain sites where music and video files can be obtained illegally, where illegal drugs can be purchased, and where child pornography can be accessed. There are no passwords: These websites operate openly. The author remains available to aid in any and all investigations, but the truth is that all these sites are common knowledge within these networks. Their linking information is no secret. The FBI, RCMP, and other law enforcement agencies already know about them. As previously mentioned, file sharing within anonymity networks is beyond legal enforcement efforts.

National Security Concerns

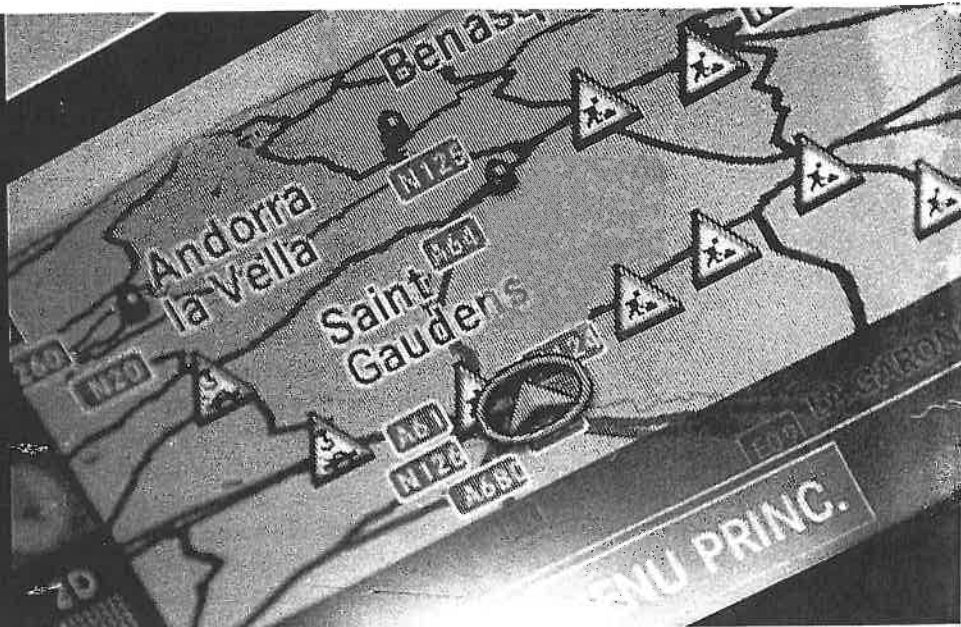
The state of the art for intelligence gathering does not involve imaging satellites or nuclear subs. The ins and outs of information systems are today more important than troop movements or missile locations. Surveilling these systems involves probing them via the Internet to learn where they are strong and where the backdoors have been left ajar. Doing this risks discovery. The target may detect the probe and link it back to the origin. If the probe is linked to IP addresses belonging to the CIA, or Halliburton, then the cover has been blown. If, instead, the probe comes from a publicly controlled anonymity network, the operation can continue even after detection. These networks do not favor one country over another. China has tried repeatedly to limit access to these networks, TOR in particular. Why, then, are so many TOR exit nodes allowed to operate openly from within mainland China? The implications are clear. Anonymity networks such as TOR are the stomping ground for any number of intelligence operations. Perhaps this is what the Navy was thinking about when it released TOR to the public.

Before Passing Judgment

If you take one thing from this extremely brief article, it should be that you should do the homework to first understand how and why these networks function before passing judgment. These are very complex networks, but they are free, easy to use, and backed by a large community willing to help new users. Everyone will find something to applaud and something to hate. ♦

Global Positioning System Technology AND THE Fourth Amendment

By Arthur G. LeFrancois



Surveillance techniques abound that were unimaginable at the time of the nation's founding. Our daily activities are more knowable by more people more quickly than was conceivable even a short time ago. How should we treat law enforcement's warrantless use of privacy-reducing technological innovations? One answer is that we simply learn to live with it. Privacy advocates respond that a hallmark of our democracy is the ability of its citizenry to lead lives free of unwarranted government monitoring. Perhaps legislation is necessary.¹ But legislation is by its nature fragile, subject as it is to cynical political manipulation or irrational risk calculation in the face of crisis. And so we turn to the constitution's prohibition of unreasonable searches and seizures: How does the current conceptual framework of the Fourth Amendment accommodate new surveillance techniques?

GPS Technology

The use of global positioning system (GPS) devices to track vehicle movements is an instructive example of the new surveillance. The global positioning system is maintained by the United States military and made available to civilian use. GPS receivers use satellite

signals to determine position, velocity, and time.² Law enforcement uses GPS technology in different ways, often surreptitiously attaching GPS units to vehicles. The GPS data are either remotely accessed through a modem or by retrieving the device. The data show where the vehicle has been since the installation and activation of the device.

Law enforcement agents are using GPS technology to investigate suspected criminals of all varieties, from cases of drugs, embezzlement, and burglary, to assault and murder.³ In response to a Freedom of Information Act request, police in one Virginia locality reported that they used GPS devices in nearly 160 cases from 2005 to 2007.⁴ Unsurprisingly, legal issues surrounding the use of GPS monitoring have begun to surface in the state and federal courts.

A Fourth Amendment Primer

First things first: The question in surveillance cases is rarely, if ever, whether the government may use a particular surveillance method. Instead, the question is simply whether the government needs to make a showing in order to justify doing what it wants. The default rule—although there are many exceptions—is that if the government is doing investigative work that the Fourth

Amendment regulates, the government needs to have obtained a warrant by establishing probable cause to believe it will find what it seeks.

As for what the Fourth Amendment regulates, those seeking its protection must show they were the object of a search or seizure. A seizure is a meaningful interference with a possessory interest.⁵ Contrarily, a search is an invasion of an expectation of privacy that is reasonable or legitimate.⁶ Reasonableness can be determined through reference to property concepts and social understandings.⁷

Only if a search or seizure is shown to have occurred may one argue that it violated the Fourth Amendment. A search or seizure can violate the Fourth Amendment because of the way that it was executed, or for lack of an underlying justification, or for lack of judicial authorization. Such violations, absent exceptions, result in suppression of the evidence obtained through the violation.

The Supreme Court and Technology

The Supreme Court has yet to rule on GPS technology's relation to search and seizure jurisprudence—whether installing a GPS device and/or accessing it implicates search or seizure protections

such as the probable cause and warrant requirements. But the Court's Fourth Amendment jurisprudence has set the stage for analysis.

In the late 1960s, the court, in *Katz v. United States*, moved from a property-related treatment of searches to a privacy-oriented conception that defines a search as an invasion of a reasonable expectation of privacy.⁸ The court decided that the government should have obtained a warrant before transmitting and recording the defendant's end of a telephone call made from a telephone booth. At the time, this seemed like quite a victory for privacy proponents.

But four years later, in a case called *White*, this new conception of "search" failed to cause the court to prohibit the warrantless transmitting of a conversation between a defendant and a government agent in the former's home. The court's theory, which antedated its earlier move from trespass to privacy analysis, was essentially that citizens assume the risk that those they voluntarily speak with might be government agents.⁹ Because no reasonable expectation of privacy was invaded, no search had occurred. Justice Harlan, who had crafted the privacy test in his concurrence in the *Katz* case, dissented, concerned as he was about the chilling effects of secret surveillance.¹⁰

Twelve years after *Katz*, the court determined that we do not have a legitimate expectation of privacy in the telephone numbers dialed from our home telephones, since we "voluntarily" turn over this information (the numbers dialed) to a third party (the phone company).¹¹ Hence, the government needs no warrant to obtain these numbers from the telephone company through company installation (on company property, at government request) of a special device (a "pen register") that records the numbers. Justice Marshall dissented, arguing that the legitimacy of privacy expectations should depend on the "risks [we]

should be forced to assume in a free and open society."¹²

In these early privacy cases, the court was taken with the notion that if a person knowingly exposed information to the public—even if the public was the telephone company with whom one had to do business if one wanted a telephone—then one could not reasonably expect that information to remain private, even from the government.¹³ Further, talking to an acquaintance in our home entailed assuming the risk that we were, effectively, talking to the government. But "secret" surveillance, as in *Katz*, was thought to be another matter. In *White*, the thinking went, one of the conversational participants was engaged in the monitoring activity; in *Katz*, neither was.

In the 1980s, the court decided two cases involving the use of "beepers" to track the movements of canisters in vehicles. Beepers are the oldest electronic tracking devices.¹⁴ They emit radio signals that can be picked up by receivers. Unlike GPS devices, beepers do not record where they have been. In *United States v. Knotts*, the court determined that the use of a beeper was not a search (did not invade a legitimate expectation of privacy), on the theory that the radio signals simply aided the agents' visual surveillance, and the surveillance was limited to tracking the canister along its journey on public highways to outside a private cabin.¹⁵

In *United States v. Karo*, the court decided that transferring a "beeped" canister to the subject of an investigation was neither a search (because it created only a "potential" for an invasion of a legitimate expectation of privacy) nor a seizure (because it worked no meaningful interference with a possessory interest).¹⁶ But the court held that monitoring a beeper in a private residence in a setting not open to visual surveillance invades a legitimate expectation of privacy and so is a search.¹⁷

In *Dow Chemical Co. v. United States*, a case involving aerial photography that failed to give the court constitutional pause, the court returned to the enhanced sensory faculties theme, warning that "[a]n electronic device to

penetrate walls or windows . . . would raise very different and far more serious questions."¹⁸ *Kyllo v. United States* subsequently treated thermal imaging of a home from a location in the street as a search. *Kyllo* was concerned about the employment of a device not in general public use that sought to reveal what would otherwise be unknowable without an entry.¹⁹

Doctrinal Challenges

There are thus a number of Fourth Amendment doctrinal obstacles to privacy preservation in the GPS context. As to the seizure question, it has proved difficult to show that the mere installation of a GPS device (without, say, removing the car to another location or delaying the owner's use of it) or extracting data from the device is a seizure—a meaningful interference with possessory rights—particularly if the device is installed and removed while the vehicle is on public property.

As for the search question, a number of doctrinal challenges arise. These include the idea that what I knowingly expose to "the public," perhaps including my vehicle's movements, cannot simultaneously be the object of a search; enhancement of ordinary senses analysis (if GPS observations could have been made by visual surveillance, there may be no search); and commonness of surveillance device (if the surveillance device was of a kind in general public use, there may be no search).

There is an additional problem. Courts sometimes accept warrantless surveillance methods that they might reject if more widely used. Judge Richard Posner, in an opinion allowing warrantless GPS installation and monitoring, besides noting that the police had "abundant grounds for suspecting the defendant," considered the possibility of "wholesale surveillance" of thousands of vehicles and deferred the question of whether such mass GPS surveillance would qualify as a search.²⁰ The Supreme Court has reacted similarly to the mass surveillance question.²¹ What might not pass muster en masse seems to go unchecked in relative isolation.

Arthur G. LeFrancois is a professor at Oklahoma City University School of Law, where he teaches criminal law, criminal procedure, and jurisprudence.

The Future

A number of approaches are worth considering in overcoming such doctrinal obstacles in the GPS context. First, we might ask whether, if GPS monitoring were unregulated by the Fourth Amendment, privacy would decrease to levels "inconsistent with the aims of a free and open society." This approach to assessing surveillance methods was suggested 35 years ago by Professor Anthony Amsterdam.²² Such a standard is consistent with an effort to recognize the normative component of "legitimate" expectations of privacy, although it obviously produces no bright line. The approach is consistent with concerns expressed by Justices Harlan and Marshall, among others.²³

Under such an approach, we might ask in new surveillance (and perhaps other) cases, not whether a person reasonably expected privacy, but whether a person reasonably expected privacy vis-à-vis the government.²⁴ Although it may be true that leaving garbage by the curbside,²⁵ traveling on public roads, or calling someone exposes information to others, maybe we ought to be able to reasonably expect that the person rooting through our garbage, monitoring every movement our vehicle makes, or recording a telephone number we dialed is not a government agent acting without a warrant. Although a partially open hotel room bathroom window might invite a peeping Tom, perhaps it ought not invite a warrantless peeping Uncle Sam (or his state cousin).²⁶ Of all of these privacy-imperiling scenarios, GPS monitoring would appear to be near the top of the list.

Second, we could seek to make more robust the older trespass view of search doctrine, and characterize as searches surveillance methods that either invaded privacy or involved trespass, however "technical."²⁷ The idea would be to regain some of the "bright-line" advantages of a property-oriented view of searches without losing protection in cases of sophisticated surveillance that involve no trespass.

Third, we might focus on the quantity of information gleaned through GPS monitoring, and determine that it is so invasive of privacy interests that

Fourth Amendment protection is warranted. This is the approach of Professor Renée McDonald Hutchins.²⁸ Her analysis seeks to directly confront the privacy challenges of GPS monitoring without revolutionizing Fourth Amendment jurisprudence.

Fourth, some federal courts, addressing an issue left unresolved in *Knotts and Karo*,²⁹ have treated installation plus monitoring of beepers as a search. Some have required a warrant,³⁰ while others have held that warrantless beeper use is acceptable, as long as probable cause exists.³¹ GPS devices, of course, are much more intrusive than beepers.

Finally, some state courts are treating monitoring of electronic tracking devices as searches requiring warrants under their state constitutions.³² These courts, as the final arbiters of the meaning of their state laws, provide privacy protection where an uncertain federal constitutional jurisprudence has not clearly done so. Meanwhile, the uneasy relationship between privacy and increasingly intrusive innovation continues. ♦

Endnotes

1. See Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004).
2. Peter H. Dana, Global Positioning System Overview, www.colorado.edu/geography/gcraft/notes/gps/gps_f.html (last visited March 28, 2009).
3. Ben Hubbard, *Police Turn to Secret Weapon: GPS Device*, WASH. POST, Aug. 13, 2008, www.washingtonpost.com/wp-dyn/content/article/2008/08/12/AR2008081203275.html.
4. *Id.*
5. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).
6. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
7. *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978).
8. 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
9. *United States v. White*, 401 U.S. 745, 749-50 (1971).
10. *Id.* at 787-90 (Harlan, J., dissenting).
11. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).
12. 442 U.S. at 750 (Marshall, J. dissenting).
13. See also *United States v. Miller*, 425 U.S. 435, 440 (1976) (bank records); *Couch v. United States*, 409 U.S. 322, 335-36 (1973) (taxpayer records held by accountant).
14. CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* 7 (2007).
15. 460 U.S. 276, 282 (1983).
16. 468 U.S. 705, 712 (1984).
17. *Id.* at 714.
18. 476 U.S. 227, 239 (1986).
19. 533 U.S. 27, 40 (2001).
20. *United States v. Garcia*, 474 U.S. F.3d 994, 998 (7th Cir. 2007).
21. *Knotts*, 460 U.S. at 283-84.
22. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).
23. See *White*, 401 U.S. at 786-90 (Harlan, J., dissenting); *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).
24. See Dolores A. Donovan, *Informers Revisited: Government Surveillance of Domestic Political Organizations and the Fourth and First Amendments*, 33 BUFF. L. REV. 333, 345, 363-65 (1984).
25. *California v. Greenwood*, 486 U.S. 35 (1988).
26. *Ponce v. Craven*, 409 F.2d 621, 625 (9th Cir. 1969) (if habeas petitioner had not wanted to be seen or heard by police, he could have closed bathroom blinds and spoken more softly).
27. See David P. Miraldi, Comment, *The Relationship Between Trespass and Fourth Amendment Protection After Katz v. United States*, 38 OHIO ST. L.J. 709, 732 (1977). Although *Rakas* says that property concepts are relevant to privacy analysis (439 U.S. at 143 n.12), *Karo* says that physical trespass is only "marginally relevant" to Fourth Amendment analysis (468 U.S. at 712-13).
28. *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 456-60 (2007).
29. *Knotts*, 460 U.S. at 279 n.*; *Karo*, 468 U.S. at 713-14.
30. *United States v. Bailey*, 628 F.2d 938, 944-45 (6th Cir. 1980) (warrants invalid for lack of termination date).
31. *United States v. Moore*, 562 F.2d 106, 112-13 (1st Cir. 1977); *United States v. Shovea*, 580 F.2d 1382, 1387-88 (10th Cir. 1978).
32. *State v. Jackson*, 76 P.3d 217, 223-24 (Wash. 2003) (GPS device); *State v. Campbell*, 759 P.2d 1040, 1049 (Or. 1988) (radio transmitter).