VIEWPOINT

Anticircumvention Rules: Threat to Science

Pamela Samuelson

Scientists who study encryption or computer security or otherwise reverse engineer technical measures, who make tools enabling them to do this work, and who report the results of their research face new risks of legal liability because of recently adopted rules prohibiting the circumvention of technical measures and manufacture or distribution of circumvention tools. Because all data in digital form can be technically protected, the impact of these rules goes far beyond encryption and computer security research. The scientific community must recognize the harms these rules pose and provide guidance about how to improve the anticircumvention rules.

Recent legislation in the United States and Europe whose ostensible purpose is to protect copyrighted works from pirates is being used to inhibit science and stifle academic research and scholarly communication. The threat to science is illustrated by strong-arm efforts of the Recording Industry Association of America (RIAA) and the Secure Digital Music Initiative (SMDI) Foundation to use the anticircumvention provisions of the Digital Millennium Copyright Act (DMCA) to suppress publication of a paper by Edward Felten of Princeton University's Computer Science Department and several coauthors (*1*). Felten's paper described weaknesses in digital watermarking technologies that RIAA and SMDI hoped to use to protect commercially distributed digital music (*2*). RIAA and SDMI asserted that the researchers could not publicly disclose details of their research without violating the DMCA (*3*). Unfortunately, such an assertion must be taken seriously because all too often in recent years, when courts have perceived a conflict between intellectual property rights and free speech rights, property has trumped speech (*4*).

Computer security and encryption researchers are far from the only scientists who have reason to fear the DMCA. Any data in digital form can be protected by encryption and other technical measures, and those who distribute digital data in this manner can use the DMCA to restrict what scientists or other researchers can do with the data.

The DMCA establishes several new rules to protect copyright owners. First, the DMCA bans the bypassing of technical measures used by copyright owners to protect access to their works (*5*). Second, it outlaws the manufacture or distribution of technologies primarily designed or produced to circumvent technical measures used by copyright owners to protect their works (*6*). Third, it makes removal or alteration of copyright management information (CMI) from digital copies of copyrighted works illegal (*7*). Copyright industry lobbyists persuaded Congress to adopt these rules to reassure rights-holders that when they used technology to identify their ownership rights (e.g., by digital watermarks) or to protect digital copies of their works (e.g., by encryption), pirates could not simply strip the CMI from those copies or use countermeasures to undo the encryption to facilitate copyright infringements (*8*).

The major recording industry firms who belong to RIAA plan to implant watermarks in digital recordings not only to identify their ownership rights but also to ensure that the music can only be played or copied if the watermarks authorize it (*9*). For this plan to work, the consumer electronics industry and makers of music-player software for PCs must build systems designed to read and conform to these watermarks. SDMI is the multi-industry consortium formed largely at the instigation of RIAA to develop technical standards for watermarks and compliant devices and player software. In September 2000, SDMI announced its selection of certain technologies as candidate standards and issued a public challenge encouraging skilled technologists to try to defeat these technical protection measures (*10*). SDMI even offered to pay $10,000 per broken watermark to anyone who demonstrated to SDMI's satisfaction that his or her attack had been successful.

Felten and his collaborators decided to accept the challenge, although they decided against seeking the prize money because SDMI was only willing to award it to those who agreed not to reveal how they defeated the watermarks to anyone but SDMI (*11*). Felten and his collaborators made no secret of the fact that they were writing a paper on the results of their research about the SDMI watermarks (*12*). When an executive from the developer of one of the candidate watermarks asked to see the paper, Felten sent him a draft. This executive and RIAA then tried to persuade Felten to omit from the paper certain details about the weaknesses of the SDMI technologies. Felten and his coauthors decided that these details were necessary to support their scientific conclusions. There ensued numerous conversations between representatives of SDMI and RIAA, on the one hand, and Felten, his coauthors, members of the conference organizing and program committees, and lawyers from institutions with which these persons were affiliated, on the other hand. SDMI and RIAA asserted that any presentation of the paper at a conference or subsequent publication of the paper in the conference proceedings would subject these persons and their institutions to liability under the DMCA and made clear their intent to take action against the researchers unless they withdrew the paper (*13*).

Although convinced that they would be vindicated if the matter went to court, Felten and his coauthors reluctantly withdrew the paper from the April conference out of concern about the high costs of litigation (*14*). This decision was widely reported in the press and has had a chilling effect on the willingness of cryptographers to publish the results of their research (*15*). Since then, the Electronic Frontier Foundation has agreed to represent Felten and his coauthors in an affirmative challenge to the RIAA and SDMI claim that seeks a judicial declaration that presenting or publishing this paper does not violate the DMCA (*16*).

The idea that Felten's paper violates the DMCA initially seems absurd on its face. Whatever plausibility it has is due to a broad interpretation given to the DMCA rules in a trial court decision in *Universal City Studios, Inc.* v. *Reimerdes* in August 2000 (*17*). Universal sued *2600* Magazine and its publisher Eric Corley (a.k.a. Emmanuel Goldstein) because *2600* posted a copy of a computer program, known as DeCSS, as part of its story about a young Norwegian hacker Jon Johanssen who figured out how to bypass the Content Scrambling System (CSS) used to protect commercially distributed DVD movies. Johanssen wrote DeCSS and posted it on the Web so that others could benefit from what he had learned. Universal convinced the trial judge that DeCSS was an illegal circumvention technology, the public availability of which threatened the viability of the motion picture industry (even though Universal did not produce any evidence that DeCSS had ever actually been used to make an infringing copy of the plaintiffs' movies; it was enough, in Universal's view, that the program could be used for this purpose).

School of Information Management and Law, University of California, Berkeley, CA 94720, USA. E-mail: pam@sims.berkeley.edu

After being ordered in January 2000 to take down DeCSS from the *2600* site, Corley decided to link to sites where DeCSS could be found. In August 2000, the trial judge ruled that linking also violated the DMCA and forbade posting or linking to source or object code forms of DeCSS. The judge rejected Corley's First Amendment defense because of the functionality of DeCSS and the danger that the program posed to Universal's market for copyrighted movies. Under this judge's reasoning, even an English-language version of DeCSS might violate the DMCA.

SDMI and RIAA regard Felten's paper as providing a functional recipe for circumventing the SDMI watermarks that posed dangers to the recording industry akin to those that DeCSS posed for the motion picture industry. SDMI and RIAA have not been willing to concede that writing and distributing a paper describing the results of reverse engineering of a technical protection measure are different from writing and distributing an executable program capable of defeating that measure [but for the fact that SDMI issued a public challenge to the technical community to try to break the technical protections they had devised, SDMI and RIAA would undoubtedly argue that the reverse engineering of publicly disseminated watermarking technologies, whether for academic research or for piratical purposes, violates the DMCA rule against alteration or removal of copyright management information (*18*)].

The ruling against Corley is on appeal. One can always hope that the appeals court will give the DMCA a narrower interpretation than the trial judge did and that this narrower interpretation will propagate in other cases. In the meantime, the DMCA is a cloud on the horizon for all computer security and encryption researchers, whether they operate in an academic or commercial setting, if their work has any potential application to protecting digital content.

Although the DMCA rules contain narrow exceptions for computer security and encryption research, practitioners in these fields take little comfort in them (*19*). Several prominent cryptographers submitted an amicus (friend of the court) brief in the Corley case in which they characterized the encryption research exception as "so parsimonious as to be of little practical value" as well as being based on a "fundamentally mistaken conception of cryptographic science" (*20*, *21*). It applies, for example, only if the researcher is employed or has been trained as a cryptographer, even though some brilliant breakthroughs in this field have come from amateurs (*22*). The researcher must also seek permission from affected rights-holders before trying to reverse engineer encryption technology (*23*). The exception further requires the researcher to prove that his or her research was necessary to advance the state of the art when the researcher may just be trying to understand how a technology works (*24*). In addition, the exception may be unavailable if the researcher publishes his or her results on the Internet because this will make them accessible to potential pirates (*25*). But the most fundamental point is that "the science of cryptography depends on cryptographers' ability to exchange ideas in code, to test and refine those ideas, and to challenge them with their own code. By communicating with other researchers and testing one another's work, cryptographers can improve the technologies they work with, discard those that fail, and gain confidence in technologies that have withstood repeated testing" (*20*). Encryption and computer security cannot get stronger if researchers in these fields are at risk of liability from the DMCA for merely working in their chosen field and communicating with one another about it.

The implications of the DMCA for science are not limited to computer security and encryption researchers. Virtually all computer scientists, as well as many other scientists with some programming skills, find it necessary on occasion to reverse engineer computer programs. Sometimes they have to bypass an authentication procedure or some other technical measure in order to find out how the program works, how to fix it, or how to adapt it in some way. The act of bypassing the authentication procedure or other technical measure, as well as the making of a tool to aid the reverse engineering process, may violate the DMCA.

Although the DMCA also has an exception for reverse engineering of a program (*26*), it too is narrow. It only applies if the sole purpose of the reverse engineering is to achieve program-to-program interoperability and if reverse engineering is necessary to do so (*27*). Trying to fix a bug or understand the underlying algorithm does not qualify. Information even incidentally learned in the course of a privileged reverse engineering process cannot be divulged to any other person except for the sole purposes of enabling program-to-program interoperability (*28*). Under a strict interpretation of the DMCA, a reverse engineer could not, for example, publish lawfully obtained interface information or details of the program's authentication technique in an academic or research paper.

Other evidence of the narrowness of the reverse engineering exception can be seen in the trial judge's response to Corley's interoperability defense (*29*). Jon Johanssen testified at Corley's trial that he developed DeCSS to help the Linux programmers develop a Linux-based DVD player. The judge rejected this defense for several reasons: First, DeCSS did not have as its sole purpose the achieving of interoperability because it could also be used to bypass CSS on a Windows-based system. Second, DeCSS might help achieve data-to-program interoperability, but the statutory exception only permits program-to-program interoperability. Third, even if Johanssen had been eligible for the interoperability privilege, Corley—a mere journalist—was not because he was not trying to develop an interoperable program.

Of course, any data in digital form—not just sound recordings and motion pictures—can be protected by technical measures. Those who disseminate digital data may want to restrict what researchers can do with the data. Imagine, for example, that a pharmaceutical company produces data to prove that a new drug is safe but technically protects it so that only certain tests can be performed on the data, all of which support the safety claim. A scientist who doubted the safety claim and tried to process the data by additional tests would violate the DMCA if he or she bypassed the access control system restricting use of the data (*30*).

Or imagine that this pharmaceutical firm put the data on an access-controlled Web site available only to those who agreed to licensing terms forbidding use or disclosure of the data or test results except as authorized in the license. A scientist who tried to access the data without agreeing to the license might also run afoul of the DMCA. Microsoft once posted a certain technical specification on a Web site, access to which was designed to be available to researchers only if they clicked "I agree" to a license that forbade disclosing details of the specification (*31*). A smart technologist figured out how to bypass the click-through license and posted instructions about it on slashdot.org, after which there was a heated debate about the specification on slashdot. Microsoft learned about the slashdot postings and demanded that slashdot delete these messages on the theory that they violated the DMCA's anticircumvention rules. Microsoft is surely not the only entity in the world that wants to control a wider community's use of its information and will find the DMCA a useful tool for achieving this objective.

Advances in technology now permit very fine-grained control over access to and use of information. This control has been powerfully reinforced by the DMCA, and it enables firms and individuals to engage in "privication" (i.e., "the mass distribution of information to 'authorized' users with tight control over its use") (*32*, p. 1218). This disturbing practice may well creep from one subdiscipline of science to another unless the scientific community recognizes the potential threat that privication and the DMCA pose for preservation of the norms and practices of science.

The question, then, is whether science can do something about it. I am optimistic that the scientific community can make a differ-

ence because it has been able to mobilize and make an effective case for policy change when expansions of intellectual property rights, actual or proposed, were about to have serious repercussions for science (*33*). The scientific community has played an important role in holding back a vast expansion of intellectual property rights to the contents of databases.

Back in 1996, the European Commission realized that many commercially valuable databases did not qualify for copyright protection because they exhibited insufficient creativity in selection and arrangement of data and that when databases did qualify for protection, the copyright in them did not protect the data themselves from being reselected and rearranged. So the Commission proposed a new form of intellectual property protection for the contents of databases, and in 1996, this new legal regime was mandated in the European Union. Now any person or firm that expends substantial resources in compiling data in the European Union has a legal right to prevent anyone else from extracting or reusing all or a substantial part (whatever that means) of the contents of the database for 15 years (*34*). Additional expenditures in maintaining the database will renew the term of protection, which arguably gives European data compilers perpetual rights in the data in their databases (*35*).

Although scientists in Europe seem not to have been consulted when this law was wending its way through the European Commission and Parliamentary approval process, scientists in the United States recognized that such a law posed serious problems for traditional norms and practices of science (*36*). They did not object to giving databases some legal protection but argued that the European Union database right went too far. So they organized a successful effort in late 1996 to persuade the Clinton Administration to back away from support for an international treaty to universalize the European database rules that a senior U.S. official had previously endorsed (*37*). These organizations also helped to persuade the Clinton Administration to moderate its stance on several digital copyright issues, including whether fair use would survive in the digital age, scheduled for consideration at a diplomatic conference in December 1996 (*38*). Thanks in no small part to these efforts, the treaty eventually adopted was balanced and sound.

Since 1996, the American Association for the Advancement of Science and the National Academies of Science and Engineering have been among the scientific organizations that have worked together to oppose European Union–style database legislation in Congress and in the international arena (*39*). So far they have been successful, but database bills will be back, and victory in future rounds will depend on continued vigilance.

The scientific community has not been as active about the DMCA anticircumvention rules, perhaps because the threat they posed seemed too abstract and diffuse. But now that the threat that these overbroad rules pose for science is more evident and immediate, it may be the right time to focus on the DMCA. There are at least two ways to do this. One is to submit amicus briefs in pending cases to urge courts to give narrow interpretations to these rules to mitigate the harm to science. Another is to make suggestions to Congress about how the DMCA could be modified to provide a better balance between protection for copyrighted works and protection for scientific research and communications.

One thing is certain: Better anticircumvention rules will not come about just because it is the right thing to do. This will only happen if the scientific community and others harmed by these overbroad rules are able to articulate why the DMCA rules are harmful and how legal decision makers can fix the problems with this legislation.

References and Notes

1. See, e.g., C. C. Mann, "Secure-Music Group Threatens Researchers Who Plan to Publish on Hacking Success," *Inside Magazine*, 22 April 2001, available at www.inside.com.
2. The paper was entitled "Reading Between the Lines: Lessons from the SDMI Challenge" and was scheduled for presentation at the Fourth International Information Hiding Workshop in Pittsburgh, PA, on 26 April 2001. For further details, see SDMI challenge FAQ at www.cs.princeton.edu/sip/sdmi/faq.html.
3. A copy of the RIAA letter to Felten asserting that presentation or publication of the researchers' paper would violate the DMCA is available at cryptome.org/sdmi-attack.htm.
4. See, e.g., M. A. Lemley, E. Volokh, *Duke Law J.* **48**, 147 (1999) (giving examples).
5. 17 U.S.C. sec. 1201(a)(1)(A). This provision is subject to seven exceptions, three of which are discussed in this viewpoint. For a critical commentary on the DMCA anticircumvention regulations, see, e.g., P. Samuelson, *Berkeley Technol. Law J.* **14**, 519 (1999).
6. 17 U.S.C. sec. 1201(a)(2), 1201(b)(1). Subsection (a)(2) pertains to technologies that bypass access controls and (b)(1) to technologies that bypass other technical measures (e.g., copy controls) used by copyright owners to protect their works.
7. 17 U.S.C. sec. 1202. Unlike section 1201, this rule has no exceptions for research or other legitimate purposes.
8. See WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearings on H.R. 2281 and H.R. 2280 Before the Subcommittee on the Courts and Intellectual Property of the House Committee on the Judiciary, 105th Congress (1997) (statements of Jack Valenti, Robert Holleyman, and Allan R. Adler in support of the anticircumvention rules).
9. For a concise description of the intended role of watermarks in protecting digital music in compliant devices, see the SDMI challenge FAQ at www.cs.princeton.edu/sip/sdmi/faq.html.
10. See "An Open Letter to the Digital Community" available at www.sdmi.org/pr/OL_Sept_28_2000.htm.
11. This is explained in the SDMI challenge FAQ at www.cs.princeton.edu/sip/sdmi/faq.html.
12. The facts in this paragraph are set forth in the complaint filed by the Electronic Frontier Foundation on behalf of Felten and his coauthors against RIAA and SDMI, which is available at www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_complaint.html.
13. Also challenged was a chapter of a Princeton Ph.D. student's dissertation that discussed the SDMI challenge. This student successfully defended her dissertation and, in keeping with standard practice in her field, posted the dissertation on the Internet. Out of an abundance of caution after withdrawal of the Felten paper (of which she was a coauthor) from the April conference, she removed the SDMI chapter from the Internet.
14. Felten's statement when he announced withdrawal of the paper from the April conference is available at cryptome.org/sdmi-attack.htm.
15. See, e.g., (*1*); K. Dawson, "Watermarks. . .or Freedom?," *Industry Standard*, 7 May 2001. One Dutch cryptographer, Niels Ferguson, has explained the chilling effects that the DMCA has had on his willingness to publish the results of his research at macfergus.com/niels/dmca/index.html.
16. The complaint is available at www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_complaint.html. Felten finally presented the paper at a USENIX conference on 15 August 2001. However, he and his coauthors continue to be concerned about DMCA liability for reasons set forth in court papers filed in response to RIAA's motion to dismiss the Felten lawsuit (also available on the www.eff.org). These concerns have been amplified by the recent arrest of a Russian programmer, Dmitri Sklyarov, for criminal violation of the DMCA rules because he wrote a program capable of bypassing an Adobe e-book program.
17. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).
18. The *Felton* v. *RIAA* complaint in (*12*) reflects concerns that the defendants claim that the researchers violated 1202 as well as 1201.
19. 17 U.S.C. sec. 1201(g), 1201(j). Felten may not be eligible for either privilege because the SDMI watermarks are not encryption and because the computer security exception does not apply to 1201(b), but only to 1201(a)(2). Neither privilege applies to 1202 claims.
20. Brief of Amici Curiae of S. Bellovin, M. Blaze, D. Boneh, D. Del Torto, I. Goldberg, B. Schneier, F. A. Stevenson, D. Wagner, in *Universal City Studios, Inc. v. Reimerdes*, to the Second Circuit Court of Appeals, 26 January 2001, available at eon.law.harvard.edu/openlaw/DVD/NY/appeal/000126-cryptographers-amicus.html.
21. Problems with the overly narrow and ambiguous encryption and computer security exceptions to the DMCA are discussed by the National Research Council [*The Digital Dilemma: Intellectual Property in the Information Age 174-75, Appendix G* (National Academy of Sciences Press, Washington, DC, 2000)].
22. 17 U.S.C. sec. 1201(g)(3)(B).
23. 17 U.S.C. sec. 1201(g)(2)(C). The computer security exception requires that the researcher actually get, and not just ask for, permission to defeat the technical protection measure. 17 U.S.C. sec. 1201(j)(1).
24. 17 U.S.C. sec. 1201(g)(1), (g)(2)(B).
25. 17 U.S.C. sec. 1201(g)(3)(A). The encryption researcher must also provide affected copyright owners with the results of his or her research in a timely manner. 17 U.S.C. sec. 1201(g)(3)(D).
26. 17 U.S.C. sec. 1201(f).
27. 17 U.S.C. sec. 1201(f)(1).
28. 17 U.S.C. sec. 1201(f)(3).
29. The interoperability defense is discussed in *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 211 (S.D.N.Y. 2000) (ruling on the preliminary injunction motion), 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (ruling after trial).
30. See A. W. Appel, E. W. Felten, *Comm. ACM* **43**, 21 (September 2000) (giving examples of academic research that might be illegal under a strict interpretation of the DMCA rules).
31. See J. E. Cohen, "Unfair Use," *The New Republic*, 23 May 2000 (available at www.tnr.com/online/cohen052300.html).
32. J. Zittrain, *Stanford Law Rev.* **52**, 1201 (2000).
33. The scientific community expressed doubts, for example, about the patenting of expressed sequence tags (ESTs) of DNA of unknown functionality. The U.S. Patent and Trademark Office thereafter issued new guidelines to require a known utility for patent-

ing of ESTs that substantially alleviated, even if they did not totally resolve, this threat to science from overbroad patent rights.
34. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J (L 77) 20.
35. For a critical commentary on the EU database directive and kindred U.S. legislation, see, e.g., J. H. Reichman, P. Samuelson, *Vanderbilt Law Rev.* **50**, 51 (1997).
36. See, e.g., National Research Council, *Bits of Power: Issues in Global Access to Scientific Data* (National Academy of Sciences Press, Washington, DC, 1997) (expressing concern about European Union–style database protection).
37. The role of scientific organizations in facilitating changes in U.S. policy is recounted in (*38*).
38. P. Samuelson, *Va. J. Intl. Law* **37**, 369 (1997).
39. These efforts are recounted by J. H. Reichman and P. F. Uhlir [*Berkeley Technol. Law J.* **14**, 793 (1999)].
40. I gratefully acknowledge research support from NSF grant SEC-9979852.

VIEWPOINT

Computer Networks As Social Networks

Barry Wellman

Computer networks are inherently social networks, linking people, organizations, and knowledge. They are social institutions that should not be studied in isolation but as integrated into everyday lives. The proliferation of computer networks has facilitated a deemphasis on group solidarities at work and in the community and afforded a turn to networked societies that are loosely bounded and sparsely knit. The Internet increases people's social capital, increasing contact with friends and relatives who live nearby and far away. New tools must be developed to help people navigate and find knowledge in complex, fragmented, networked societies.

Once upon a time, computers were not social beings. Most stood alone, be they mainframe, mini, or personal computer. Each person who used a computer sat alone in front of a keyboard and screen. To help people deal with their computers, the field of human-computer interaction (HCI) developed, providing such things as more accessible interfaces and user-friendly software. But as the HCI name says, the model was person-computer.

Computers have increasingly reached out to each other. Starting in the 1960s, people began piggybacking on machine-machine data transfers to send each other messages. Communication soon spilled over organizational boundaries. The proliferation of electronic mail (e-mail) in the 1980s and its expansion into the Internet in the 1990s (based on e-mail and the Web) have so tied things together that to many, being at a computer is synonymous with being connected to the Internet.

As a result, HCI has become socialized. Much of the discussion at current HCI conferences is about how people use computers to relate to each other (*1*). Some participants build "groupware" to support such interactions; others do ethnographic, laboratory, and survey studies to ascertain how people actually relate to each other. This work has slowly moved from the lone computer user to dealing with (i) how two people relate to each other online, (ii) how small groups interact, and (iii) how large unbounded systems operate—the ultimate being the worldwide Internet, the largest and most fully connected social network of them all. Just one small portion of the Internet—Usenet members—participated in more than 80,000 topic-oriented collective discussion groups in 2000. 8.1 million unique participants posted 151 million messages (*2–4*). This is more than three times the number identified on 27 January 1996 (*5*)

Computer scientists and developers have come to realize that when computer systems connect people and organizations, they are inherently social. They are also coming to realize that the popular term "groupware" is misleading, because computer networks principally support social networks, not groups. A group is only one special type of a social network; one that is heavily interconnected and clearly bounded. Much social organization no longer fits the group model. Work, community, and domestic life have largely moved from hierarchically arranged, densely knit, bounded groups to social networks.

In networked societies, boundaries are more permeable, interactions are with diverse others, linkages switch between multiple networks, and hierarchies are flatter and more recursive (*6–8*). Hence, many people and organizations communicate with others in ways that ramify across group boundaries. Rather than relating to one group, they cycle through interactions with a variety of others, at work or in the community. Their work and community networks are diffuse and sparsely knit, with vague overlapping social and spatial boundaries. Their computer-mediated communication has become part of their everyday lives, rather than being a separate set of relationships.

When computer-mediated communication networks link people, institutions, and knowledge, they are computer-supported social networks. Indeed, if Novell had not gotten there first, computer scientists would be saying "netware" instead of "groupware" for systems that enable people to interact with each other online. Often computer networks and social networks work conjointly, with computer networks linking people in social networks and with people bringing their offline situations to bear when they use computer networks to interact.

The intersection of computer networks with the emerging networked society has fostered several exciting developments. I report here on two developing areas: (i) community networks on- and offline and (ii) knowledge access.

Community Networks On- and Offline

Community, like computers, has become networked. Although community was once synonymous with densely knit, bounded neighborhood groups, it is now seen as a less bounded social network of relationships that provide sociability support, information, and a sense of belonging. These communities are partial (people cycle through interactions with multiple sets of others) and ramify through space [a low proportion of community members in the developed world are neighbors (*7*)]. Where once people interacted door-to-door in villages (subject to public support and social control), they now interact household-to-household and person-to-person (*9*).

Although the support of collaborative work was the initial purpose of the Internet (both e-mail and the Web), it is an excellent medium for supporting far-flung, intermittent, networked communities. E-mail transcends physical propinquity and mutual availability; e-mail lists enable broadcasts to multiple community members; attachments and Web sites allow documents, pictures, and videos to be passed along; buddy lists and other awareness tools show who might be available for communication at any one time; and instant messaging means that simultaneous communication can happen online as well as face-to-face and by telephone.

Systematic research on what people actually do on the Internet has lagged behind the Internet's development. After a long

Centre for Urban and Community Studies, University of Toronto, 455 Spadina Avenue, Toronto, Canada M5S 2G8. E-mail: wellman@chass.utoronto.ca