The Columbia
Science and Technology Law Review
http://www.law.columbia.edu/stlr

The 'Principles in Context' Approach to Internet Policymaking

Andrew L. Shapiro*

Since the Internet's emergence, a common inquiry in public policy circles has been the "metaphor" question. In trying to figure out what rules should apply to computer networks such as the Internet, lawmakers and policy analysts want to know: what's the right metaphor? Is content on the Internet like printed material, which is generally immune from government regulation? Or is the Internet more similar to radio or television, which traditionally have been regulated because channels of communication are scarce and expensive? Or is it most like telephones and the mail, to which the rules of common carriage have been applied, ensuring low-cost, universal service?

This reasoning by analogy is typical of how the law treats any technology at its inception: the automobile initially is governed by the law of the horse and carriage, the telephone is compared to the telegraph, television to radio, cable to broadcast, and so on. In each case, the goal is to fit a technology within an existing legal regime; it would seem odd to begin any other way. As a result, lawmakers will dutifully compare the code features of the Internet to those of other media, trying to figure out whether it is most similar to print, broadcast, or common carriage.[1]

Yet the malleability of the Internet means that it can, in some ways, resemble each of those formats – or none of them at all. Moreover, the problem with simply comparing the Internet to other communications media is that it fails to take into account the new context that this technology is fostering.

While the same might be said of any new communications medium, the Internet appears to be changing the existing social and political landscape faster and more substantially than any new technology in recent memory. Indeed, the scope of change has led observers to conclude that old rules and regulations don't work anymore and should be scrapped.

---

* Senior Advisor, Markle Foundation; A.B., Brown University, 1990; J.D., Yale University, 1995. This article is adapted from The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know (Century Foundation/Public Affairs: 1999) <see www.controlrevolution.com>.

[1] *See, e.g.*, Reno v. American Civil Liberties Union, 521 U.S. 844 (1997) (ruling that the Internet is entitled to the full First Amendment protection accorded to printed speech, as opposed to the more limited protection granted to broadcast media).

Some information owners, for example, believe that digital technology makes copyright law useless. Because the Internet is a digital, interactive, distributed network, it is easier for anyone to reproduce and instantly distribute protected material. The threat of copyright infringement is not limited to professional thieves who sell black market videos, music CD's and computer programs. Instead, owners now fear the large, anonymous mass of casual Internet users who may have few qualms about unauthorized reproduction of copyrighted material.

Owners of original works are not alone in thinking that existing law is inadequate; the government too is calling for new regulations to apply to the digital realm. For example, the F.B.I. claims that advances in encryption require new rules of access to communications for law enforcement. Concerned about potential threats to national security, the F.B.I. has urged Congress to require encryption products to be built with a "key escrow" system obliging computer users to deposit a copy of their private encryption keys with a company that would act as an escrow agent. Law enforcement officials engaged in investigation of criminal activity could obtain quick access to the plain text of messages by presenting a warrant to an escrow agent requesting an individual's deposited key.

There is a tension, then, between two competing values: (1) for the sake of consistency, apply existing rules, and (2) in light of new a technological context, devise new rules.

Thus far in the Internet's short history, both the "existing rules" approach and the "new context" approach have been tried – each with their fair share of problems. A solution to this quandary lies in finding a balance between those two approaches: a way that we might call the "principles-in-context" approach.

The essence of this idea is simple. In figuring out how a new technology like the Internet should be governed, we should not be constrained by the form of existing rules; but neither should we start from scratch in reconciling competing interests. Rather, we should borrow from time-tested arrangements to achieve efficient and just results in a different set of circumstances. This generally means taking the *principles* that underlie existing laws and rules and mapping them to fit a new context.[2] Some modification may be necessary. But generally, as the following examples should demonstrate, this approach will be more effective than either rigidly applying old rules or coming up with entirely new ones.

Children and Sexual Content

The experience of the Communications Decency Act demonstrated that governments concerned about the ability of minors to find sexual materials online may overreact and try to radically change the code of the Internet.[3] As is well known, the CDA made it a felony, punishable by a fine and up to two years in prison, to knowingly transmit "indecent" messages to anyone under eighteen years of age or to display

[2] *See* Lawrence Lessig, *Fidelity in Translation*, 71 Texas L. Rev. 1165 (1993).

[3] *See Reno,* 521 U.S. at 860, 861.

"patently offensive" messages so that they might be available to a person under eighteen. Less well known, though, was the law's safe-harbor provision—an affirmative defense that would prevent individuals from being prosecuted if they took certain steps. The safe harbor prevented prosecution of Internet users who restricted minors' access to indecent material by establishing a technological means of checking the age of those who might receive their communications—for example, with credit card verification or an adult password.[4] In essence, then, Congress attempted to encourage all Internet users—whether they ran a commercial web site or just used email or chat rooms for their own benefit—to change the way they used the Internet by changing the architecture of online interaction. Courts have properly rejected these attempts, but they have also recognized that the underlying interest, keeping certain sexual materials from children, is a legitimate public concern. The question, then, is: What principle traditionally underlies laws protecting minors in a non-digital world – and how can that principle be translated to the new context of the Internet?

In the United States, the constitutional principle is fairly clear: materials that a community deems inappropriate for minors may lawfully be kept from children so long as the free speech rights of adults are restricted as little as possible and parents retain the right to override the community's judgment with regard to their own children.[5]

This results in a variety of rules. Where a parent or other guardian is available to supervise a child, for example, no state restriction on content is needed because of the presumption that parents can best determine which materials their children should not see. Still, government can play a role. Public libraries, for example, routinely help parents to choose suitable materials by publishing lists of suggested books for different age groups. These are sometimes called "white lists" (as opposed to "black lists" of inappropriate books).

When a parent is not available to supervise a child – for example, outside the home in a commercial setting, or when a radio broadcast occurs in the afternoon – a more restrictive rule governs. The case of Sam Ginsberg, is instructive. In 1965, Ginsberg was running a stationery and luncheonette in Bellmore, Long Island. A young man walked in and asked to buy a few adult magazines that were for sale in the store. Without requiring any identification or asking his age, Ginsberg sold him the magazines. Soon thereafter Ginsberg was prosecuted by Nassau County officials and convicted for giving materials deemed "harmful to minors" to a child under seventeen. The young man, it turned out, was sixteen years old. Ginsberg was found guilty by a judge who determined that Ginsberg knew the contents of the magazines, had reason to know the young man's age, and had a legal obligation to prevent him from receiving the material. The case went all the way to the Supreme Court, which upheld Ginsberg's conviction.[6]

Today it is well-settled law that commercial intermediaries such as booksellers and movie-theater owners have an obligation to act as gatekeepers, keeping certain materials away from minors. Society relies on commercial retailers to check the age of those who

---

[4] *Id.*

[5] *See, e.g.*, F.C.C. v. Pacifica Foundation, 438 U.S. 726 (1978); *Reno*, 521 U.S. at 844.

[6] *See* Ginsberg v. New York, 390 U.S. 629 (1968).

want to obtain adult magazines and other materials. Though young-looking adults may therefore have to show identification to receive sexual content, courts have (not surprisingly) decided that this is an acceptable burden in order to protect children. Parents, if they want, can also obtain adult materials for their children.

How do these rules, and the general principle that underlies them, translate to the Internet context? White lists work just as well online as in the print world, and many libraries and other groups have created them by setting up web sites with links to materials that are appropriate for different age groups. As offline, though, this solution only works where a parent is available to supervise a child's use of the Internet. For all the other times that a minor is online, how should the child-protection principle play out?

With the Communications Decency Act, the government took the "existing rules" approach to this question and basically tried to apply to the Internet the vague indecency standards that govern radio and television. The Supreme Court struck down the CDA on First Amendment grounds and expressly rejected the government's strategy, noting that the Internet was not like broadcast. The Court added that the CDA would have prevented adults from having access to speech to which they were entitled and prevented parents from overriding the state's decision about what their children should see.[7]

An alternative strategy proposed by some civil libertarians illustrates the "new context" approach. It calls for government to recognize the novelty of the Internet and to therefore refrain from regulating it, instead allowing parents to install indecency-blocking software on their home computers (such as CyberPatrol, CyberSitter, and NetNanny). If these tools were more precise in excluding only clearly inappropriate material, this might be a promising solution. But thus far, in-depth testing of these tools has shown that they block a substantial amount of legitimate content. They also usually prevent users (i.e., parents) from determining exactly what is screened out, because of concerns about proprietary methods of filtering.[8] Most importantly, since these software packages are costly and can be difficult to use, one cannot assume that they would be widely adopted.

The "principles-in-context" approach asks: what about having commercial intermediaries online replicate some of the role that Sam Ginsberg plays offline? Congress appears to have assumed that there are no such middlemen on the Internet. Frustrated by the inability of law enforcement officials to identify pornographers who use "anonymous remailers" to distribute their materials online, or their inability to hold Internet users in other jurisdictions accountable for their acts of defamation or fraud, the Internet's lack of traditional top-down controls has made Congress uneasy. That's why, with the CDA, it forced individuals themselves to develop and use interfaces to screen out material that might be harmful to minors – a burden that the Supreme Court found

[7] *Reno*, 521 U.S. at 893, 904.

[8] A number of valuable critiques of filtering software have been produced, including Electronic Privacy Information Center, "Family Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet," at http://www.epic.org/reports/filter-report.html, and American Civil Liberties Union, "Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet," at http://www.aclu.org/issues/cyber/ burning.html.

both technically impossible and constitutionally problematic.[9] But Congress and the Court were failing to account for the malleability of the Internet, which means that intermediaries could probably be found to handle this job. The question is whether, as a matter of law and policy, we would want them to do so.

On the one hand, asking intermediaries to assist in keeping sexual materials from children could be more efficient and speech-protective than the government's CDA strategy, since individual speakers would not have to bear the cost of screening material. On the other hand, it might be cheaper, more precise, and less cumbersome than voluntary use of blacklist programs. Who, though, would this gatekeeper be?

The most appropriate intermediaries to deputize might be the manufacturers of browser software – Microsoft and Netscape – since it is their technology that allows a Internet user to encounter material stored on a distant web server. In a sense, like Sam Ginsberg, they hand material over to people. Therefore, they might be required to give adults access to the full Internet while steering minors to the equivalent of the children's section in a store.[10]

How would they do this? After all, Ginsberg can tell pretty easily who is a minor and who is not (or at least who needs to be asked for ID), but Microsoft and Netscape have no idea how old their customers are. They could find this information out easily, though, using a technology known as a digital certificate – a kind of virtual ID card that can be embedded into browser software to let Internet users identify themselves during online transactions. The browser companies could use digital certificates to establish one simple fact: whether a user was a minor or an adult. (To protect the privacy of the user, no other information would be collected.)

Once they had this age information, Microsoft and Netscape would know who was entitled to use a regular browser, which would give unrestricted access to the Internet, and who was only entitled to a new product called a "kid browser." An adult who established her age once online – with a credit card or other form of ID – would download a regular browser to be used from there on. The default browser available on new computers, though, would be a kid browser. Minors, therefore, would have to use a kid browser (unless their parents gave them access to a regular browser, as a parent can do with any magazine in Ginsberg's store).

Who would decide what one could see with a kid browser? In physical space, Sam Ginsberg makes this judgment call, but (fortunately) there would be no way for the browser companies to do so with an endless Internet to evaluate. So other strategies

---

[9] In 1998, Congress tried a more subtle form of code regulation, one that came closer to recognizing that there might be middlemen on the Net: It passed the Child Online Protection Act (COPA), a more narrowly tailored Internet indecency law, known informally as CDA 2, which applied only to commercial web sites (and used a more limited definition of what material was supposed to be restricted). COPA has been preliminarily enjoined by a federal judge on the grounds that it is likely unconstitutional. *See* Pamela Mendels, *Setback for a Law Shielding Minors From Adult Web Sites*, N. Y. TIMES, February 2, 1999, at A12. Internet service providers, it should be noted, have been effectively immunized from liability for indecent content transmission by section 230 of the Communications Decency Act, which is still good law. *See* 47 U.S.C. § 230(c)(1) (1996).

[10] *Cf. Ginsberg*, 390 U.S. at 644-645 (1968).

would have to be considered. One would be to have kid browsers give access to a variety of white-list sites online; this would make web access for minors analogous to visiting a children's library. A more permissive strategy would be to have kid browsers give access to all sites except those voluntary blocked by purveyors of adults materials; but this might be subject to abuse or just reasonable disagreement about what's appropriate for children. The best option might be to create one kid browser for each strategy and let parents decide which they think is most appropriate for their own children, depending on their age and maturity.[11] (Kid browsers could even be made age appropriate, so that a 15-year-old could be given broader access by her parents than a 12-year-old would get.)

Requiring companies like Microsoft and Netscape to create kid browsers would simply be a way of recognizing that commercial middlemen have a role to play in protecting the public interest. Like Sam Ginsberg, they owe something to the community. Mapping Ginsberg's role to the context of the Internet would take some modification, though, in ways that actually turn out to be constitutionally preferable. Unlike Ginsberg, the browser companies would not have to make any judgment about what was appropriate for children. They also would not be subject to criminal liability if minors did obtain access to inappropriate materials (the requirement that they create kid browsers would simply be a civil regulation).

With a variety of kid browsers to choose from (and the option of overriding the system to let their children use an unrestricted browser), parents would have more control than they generally do over what their children see. For adult users, having to establish their age once to download an unrestricted browser would be a very minor obligation. (Compared to offline interactions, it would be less burdensome for young-looking adults who are constantly required to show ID to get access to adult materials.)[12] A kid browser scheme would be preferable in terms of cost, effort, and efficiency to having parents

[11] The white-list kid browser might also allow adult users to add web sites to the list of acceptable destinations.

[12] Requiring Internet users to take affirmative steps to establish their adult status – and, by implication, their desire to see more than kiddie fare – could present privacy problems and other constitutional concerns. Unlike the real space burden of showing identification in order to obtain adult material, cyberspace verification would seem to require a digital record and storage of the adult's preference. The Supreme Court has indicated the constitutional problems with such an approach. In *Denver Area Ed. Telecom. Consortium, Inc. v. FCC*, 518 U.S. 727 (1996), the Court struck down provisions of a cable regulation statute that would have required adult viewers to submit a written request for access before they could receive 'patently offensive' but protected programming in their homes. *Id.* at 754-755. The majority found that this written notice requirement would "restrict viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the 'patently offensive' channel." *Id.* at 754. The Court relied on *Lamont* v. *Postmaster General*, 381 U.S. 301, 307 (1965), which found unconstitutional a regulation requiring recipients of Communist literature to notify the Post Office that they wished to receive it. *See also* Lawrence Lessig, Code and Other Laws of Cyberspace 176-177 (1999), wherein Lessig articulates the constitutional infirmity of content regulation schemes that place the burden of identification on the adult, rather than on the child or the child's parents, as a means to access material deemed inappropriate for kids. These concerns might be cured by allowing an individual to establish her age anonymously through a third party, so that no one would know she had downloaded an adult browser.

install their own blacklist software. And it would certainly be constitutionally superior to the CDA, since adults would have unrestricted access to content on the Internet.[13]

Expectations of Privacy

The value of applying principles in context can be seen also in the arena of encryption, secrecy, and law enforcement. A fundamental principle of America's constitutional system is that when government officials investigate criminal activity, they must also respect citizen privacy. This principle has traditionally been expressed in specific rules: law enforcement officials may intercept private communications if they follow certain procedures. To wiretap a phone and listen in on a conversation, police must prepare a sworn statement explaining why they have probable cause to investigate a person, and a magistrate must approve the search. Failure to comply with this process may cause a court to suppress any evidence obtained. Thus, citizens can, at least in theory, rely on courts to protect them if law enforcement officials cut corners.

Does this traditional set of rules map well to the arena of digital communications? Most strong encryption advocates say yes, arguing that law enforcement can still do its job under "existing rules." Law enforcement officials, of course, disagree, noting that even if they get a warrant and intercept a message, it will be undecipherable if scrambled with strong encryption. Here, then, the police take the "new context" approach, arguing that encryption technology is changing the dynamics of secrecy so much as to require a new regulatory arrangement. The prime feature of that scheme, noted earlier, is key escrow: requiring encryption users to make available an extra set of deciphering keys so that police can obtain access to encrypted communications.

But is *this* a rule that fairly applies the time-tested principle of compromise between citizen privacy and law enforcement? At first, it may seem so. Yet when we consider the context of the Internet, it becomes clear that the government's proposed modification runs afoul of the original principle.

It all has to do with our changing expectations of privacy in remote communications. Law enforcement says key escrow is no different than an analog (i.e., non-encrypted) telephone wiretap, since both require a warrant and both are subject to some theoretical possibility of abuse. In fact, it is probably easier to wiretap a phone than it is to get unauthorized access to an escrowed key. Yet precisely because a wiretap can be done by anyone with some cheap surveillance equipment and a little know-how, most users of

[13] Since *Butler v. Michigan*, 352 U.S. 380 (1957), in which the Supreme Court struck down a Michigan statute making it an offense to provide obscene materials to the general reading public, the Court has protected adult access to constitutionally protected but pornographic material on the grounds that it is constitutionally impermissible "to reduce the adult population…to…only what is fit for children." *Id.* at 383. Thus any regulation of Internet content, to survive constitutional scrutiny, will have to protect access for adults. *Cf. Denver Area Educational Telecommunications Consortium, Inc. v. F.C.C.*, 518 U.S. 727. (1996) (stating that despite the fact that nothing short of an absolute ban could prevent a child from gaining access to patently offensive material on cable channels, "We have not, however, generally allowed this fact alone to justify 'reducing the adult population …to …only what is fit for children.' "). *Id.* at 759 (citing Sable Communications of California v. F.C.C., 492 U.S. 115 at 128 (1989) (further citations omitted)).

analog telephones don't have a high expectation of privacy when it comes to traditional phone calls. Given the content of a typical telephone conversation, this is not surprising.

The Internet is different. Users of computer networks are likely to transmit not just everyday chat, but sensitive personal and commercial information such as financial records, medical files, legal documents, and the like. Even when phone users do speak about such matters, their speech is ephemeral. By contrast, Internet users often send *and store* sensitive documents on computer networks. With strong encryption, they can do so with true security. Without it, interlopers – be they law enforcement officials or private spies – can obtain access not just to gossip but to highly sensitive information. The difference between key escrow and a wiretap, then, is that the expectations of privacy in the former context are substantially higher than in the latter.

To their credit, law enforcement officials are correct about at least one thing: strong encryption does give individuals more power to keep secrets from government (and others) than they have otherwise had. Yet because the context of the Internet means that users are substantially more vulnerable in terms of the information that is at stake, depriving them of strong encryption would actually give them *less* control and security – and less power relative to government – than they have previously had in other contexts.

No viable rule has emerged that would perfectly replicate the original compromise between law enforcement and citizen privacy. For now, then, a choice must be made: in translating the law enforcement/privacy principle to a new context, do we choose a rule that favors individuals or one that favors government?

Against the backdrop of an increased need for privacy in remote communications, the right thing to do is to err on the side of giving individuals more security. That means government should either scrap key escrow or defer to cryptography experts who would assist in creating an escrow architecture oriented more toward safeguarding privacy than those that have been proposed. (The suppleness of code, after all, means that it can be altered not just in regressive ways, but in positive ways.)

This is not to say that strong encryption does not present problems for society. Beyond its use by terrorists and child pornographers, strong encryption could be used more mundanely to hide economic activity that should by law be taxed. (Radical libertarians love the notion of making untraceable electronic deposits to off-shore bank accounts, frustrating the efforts of tax collectors.) The consequences would be felt by everyone: every tax dollar not collected, after all, has to be made up by innocent taxpayers or accounted for with cuts in public services.

Yet the answer to such a potential dilemma, and to others, is not to reflexively deny individuals strong encryption, but to pursue other methods of law enforcement. It is, in fact, particularly in the interest of encryption proponents to work with investigators to figure out ways in which our communities can be protected without having institutional powers unnecessarily restrict privacy or the use of emerging technologies. In fact, with its own use of new technology, law enforcement should have other investigative advantages that will help it to enhance public safety without diminishing privacy rights.

Creative Breathing Room

In the case of copyright and creativity, applying principles in context is again crucial to finding the right rule to reconcile competing interests. The principle at stake is also one of constitutional dimensions: how do we encourage and reward the creation of original works while at the same time allowing the public to benefit from those creations? Traditionally, copyright law has given authors and other creators a limited exclusive monopoly in their work so that they can charge for its use and make a living as writers and artists. This in itself is beneficial to society. Yet the law has also recognized the need, in an open society, to give the public certain limited opportunities to use copyrighted work – for example, for personal use or to critique a work. It recognizes an equilibrium between rights of property and free speech.

As mentioned earlier, powerful copyright owners in the entertainment, publishing, and software industries believe that digital technology, including the Internet, is creating a new set of circumstances that could deprive them of their most lucrative assets. Smaller companies and individual writers and artists also are concerned that their source of income may be jeopardized. These fears are justified, because new technology does give individuals the ability to copy and distribute protected materials with far greater ease than before, usually with impunity. Adhering to the "existing rules," then, is probably inadequate.

Yet the new rules of information protection now being put into place by government and copyright owners are too broad in scope. They are expanding copyright law and changing the code of digital technology to require use of information protection schemes – such as trusted systems and clickwrap contracts – that could unduly limit the rights of users, while making more and more information available only on a pay-per-view basis.[14] Every information transaction that uses digital technology might be regulated, monitored, and controlled.

The rules for this new context, in other words, are too perfect. In contrast to the balance underlying copyright law, there is no lenience that allows for personal and critical uses of protected works – in other words, no guarantee of fair use.[15] The timeless compromise between protecting works and making them publicly available is therefore in danger of coming undone. These new rules respect one element of the digital context: the ability of the Internet to be a giant copying machine. But they ignore another: the sometimes unforgiving and unpredictable precision of technology. A good example of

[14] Anyone who has used a software program or gone online in search of proprietary information has undoubtedly confronted the ubiquitous computerized form agreements know as "clickwrap contracts." These contracts limit the ways that information can be used. By going beyond the protection provided by copyright law. Usually they contain hundreds of lines of fine print followed by an O.K. button that you are supposed to click to signal you assent. An even more sophisticated and effective tool for protecting information is known as "trusted systems." This technology regulates how digital information is used: how many times it can be viewed, whether it can be duplicated, and so on. It seeks to tip the balance of control over creative works from the user back to the owner. The enforcement is built into the code itself: the owner of the material can simply program the material so that it cannot be copied when it is displayed or distributed. *See* Mark Stefik, *Trusted Systems*, SCI. AM., Mar. 1997, at 4.

[15] With the surveillance of trusted systems, there would appear to be no wiggle room to let pass what would otherwise be *de minimis* uses.

this is filtering technology. By allowing us to select and narrow the information we are exposed to online, filters such as My Netscape, My AOL or news services that send to your email box only those stories on topics you have previously selected, can unexpectedly cause the benefits of personalization to be squandered. The convenience of being able to filter out some of the endless information the Internet makes available can have the unintended side effects of ignorance and narrow-mindedness. The precision of such technological filters makes possible the near-absolute avoidance of any information not pre-selected to be included in our online world, leaving us with a loss of diverse experience and a flattened perspective. Likewise, the new information protection schemes can backfire and jeopardize the important goal of preserving copyright *and* a rich public domain.

The remedy to this situation lies in modifying the rules of information protection to allow for some of the breathing room that has always been a part of copyright law. Applying this principle in context means that the code of trusted systems and clickwrap contracts must be altered to preserve the ability of individuals to copy and otherwise use a work for a few socially beneficial purposes – parody, commentary, personal use – that would not unduly interfere with society's overall goal of encouraging creativity.

Government should recognize the importance of this breathing room, by adopting a rule analogous to fair use that might be known as "fair hacking" or "fair breach." This would give individuals the right in certain limited situations to circumvent technological protections of information or to ignore the provisions in clickwrap contracts. If legislatures fail to enact such exceptions, courts should find that constitutional principles, including the First Amendment, require that they be recognized.

Conclusion

The "principles in context" approach then, is a two-fold process of identifying the principles at the core of time-tested legal rules and ensuring that these principles not only survive, but continue to work. Taken out of the context from which they emerged, old laws will do little to preserve the constitutional principles they embody if they are simply grafted on to new and uncharted territory, such as that created by the Internet. The meaning of law is determined in part by the surrounding circumstances and conditions at the time of its adoption. As circumstances and conditions change, so must the rules that govern them. But, in our effort to respond to new contexts, we should not forsake the values and balances that have shaped our legal tradition. To do so would be to sacrifice principles in the name of novelty. Essential to the "principles in context" approach is that our fundamental laws-- of free speech, privacy and property—do not just symbolize our values. They must actually carry them into the future. To do this, the core principles must be exhumed from the old rules and the rules reconstructed to account for and accommodate the new context that the Internet presents.