On 24 May 1844, Samuel Morse telegraphed the words “What hath God wrought?” from Baltimore to Washington on a newly created telegraph line. Looking forward more than 170 years later, we might ask ourselves what the Internet and the World Wide Web have brought to our modern societies. The ability to access countless amounts of information provided by a significant fraction of the Internet population (about 3.5 billion users) has contributed to rapid sharing of news, scientific results, social discourse, online archives, and libraries, to say nothing of countless transactions in electronic commerce. The freedom to speak and to hear lies at the heart of these benefits. They’re enshrined in the American Bill of Rights under the First Amendment to the Constitution of the United States and in the United Nations’ Universal Declaration of Human Rights.

At the same time, we can’t ignore the consequences of offering a digital megaphone to every Internaut, particularly those who might not have a society’s best interests in mind. Headlines tell us that malware abounds (the most recent as of this writing is the WannaCry ransomware virus that encrypts users’ data until a ransom is paid to obtain the key). That there are users of the Internet who have malevolent intent is indisputable. This extends to nation states and organized crime as well as self-styled hackers. The recent elections in the US and Europe opened up opportunities for the production of so-called “fake news” and promulgation of “alternative facts” intended to disrupt thoughtful dialog and democratic processes. There’s a price to pay for the freedom that the Internet offers, and it seems timely to ask whether we’re paying an unnecessarily high price and, if so, what might be done to change the equation without losing the high value that freedom of expression confers.

Spam is with us daily and some estimates are that spam makes up 99 percent of all email sent. Filters have dealt with much of the email spam problem. Central filtering of spam in cloud-based systems benefits all users, but especially those where access speeds are low or costs are high. Mail spoofing is too easy and various attempts to control it through DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting, and Conformance (DMARC), and Sender Policy Framework (SPF), for example, have had limited success. Phishing attacks continue to be a popular method for inducing naive (and sometimes experienced) users into ingesting malware, leading to more serious breaches of security.

Malware is a serious problem. That there are exploitable bugs in deployed software is a fact of our networked world. Although patching can help, it isn’t uniformly applied where needed. As the Internet of Things (IoT) grows, the effects of bugs, malware, and denial-of-service attacks will be more acutely felt. While there doesn’t seem to be a guaranteed cure for these problems, we might consider means by which users can more reliably determine with whom or what they might be interacting. That’s also important for IoT devices that shouldn’t interact with other devices or systems that they can’t reliably identify. The integrity and origin of new software downloads must be strongly authenticated.

In some ways, the IoT problem seems more containable, since certain devices probably shouldn’t be interacting with very many others or, if they do, then perhaps through a smaller number of verifiable intermediaries. Even here, there are challenges. New users of IoT devices

Vinton G. Cerf • Google
will need to be authenticated to authorize control of the devices and their data. Some users need to be de-authorized (such as guests coming and departing from residences). The mechanics of these processes will determine the level of inconvenience they impose and the degree to which the processes will be adopted regularly by residential users and private and public sector operators.

It seems inescapable that users must have means to strongly identify themselves to other parties for purposes of enabling various kinds of transactions. Webpages with “comment” features might insist on some form of authentication, even if that information isn't shared publicly. Anonymous expressions might require manual reviewing and filtering or might not be permitted in some instances. There are, of course, circumstances in which anonymity is prescribed — whistleblower reports, for example.

While we have yet to determine what, exactly, is the online moral equivalent of shouting “Fire!” in a crowded theater, it seems clear that societies that are significant users of online resources need a way to cope with a wide range of harms that malevolent users might visit upon others. The need is transnational in scope, and users aren’t exempt from responsibility. Adopting safe networking practices (supported by cooperating online services companies) should be a high priority, and providing technical means to implement them should be the business of the computing and networking community. Finding mutually supportive legal agreements between nations to sanction harmful online behaviors will be a challenge worth exploring.

Vinton G. Cerf is vice president and chief Internet evangelist at Google, and past president of ACM. He’s widely known as one of the “fathers of the Internet.” He's a Fellow of IEEE and ACM. Contact him at vgerf@gmail.com.