



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 6, No. 41, 10/15/2007. Copyright © 2007 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### New Internet

Internet Protocol version 6, or IPv6, is the latest edition of the platform that supports the entire Internet, and will replace version IPv4, which has existed for 20 years. To date, though, the United States lacks a single, organized effort to implement IPv6. The federal government has set a deadline of June 30, 2008 for all government agencies to be IPv6-compliant, and IPv6 will dramatically impact the privacy and security landscape for all organizations. But so far, the switch from IPv4 to IPv6 has been slower to start than originally anticipated. The authors discuss a range of relevant issues, including a list of IPv6 issues for privacy attorneys and measures organizations should be taking now to address IPv6 privacy and security concerns.

## IPv6: Data Security and Privacy Concerns in the New Internet

By MICHAEL W. HUBBARD, CISSP, AND TOM PATTERSON

**“T**he implementation of IPv6 is important to the technological competitiveness of Europe. However whilst the rapid deployment of IPv6 should be encouraged, this should not be at the expense of safeguarding certain important principles.”

*IPv6: Legal Aspects of the New Internet Protocol (Euro6IX 2005)*

“As a result, all organizations will need to develop security plans and policies for dealing with IPv6 traffic, regardless of their decisions whether and when to transition to IPv6.”

“These realities, coupled with the fact that bad actors are rapidly adopting IPv6 and are already using it to initiate attacks and hide malicious processes and communications, suggest that all organizations should develop explicit plans to provide, or prevent, IPv6 communications. Failure to do so will create the real potential that IPv6 will appear and be used on an organization network either by accident or for malicious intent.”

U.S. Department of Commerce, National Institute of Standards and Technology, National Telecommunications and Information Administration, *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)* (January 2006)

Suppose that a manufacturer could instantly locate and track every piece of product in stock in real time, whether the item was on a shelf in Beijing or a truck in Boston.

Imagine that within seconds of a crash on the Interstate, police and rescue crews already had critical information about the wreck and the vehicles involved. Or imagine that monitoring sensors on a bridge can communicate in real-time with a bridge safety officer.

Such advances are right around the technological corner, thanks to IPv6, the new Internet protocol—the language that allows devices to communicate via the Internet. IPv6 technology will allow for a more powerful, more flexible, more portable Internet. Businesses stand to benefit greatly from this next-generation Internet.

But user privacy and data protection remain key concerns with respect to IPv6, just as they are with the current protocol version, IPv4. Protecting the privacy of Internet users is essential to the success of IPv6. Commentators on both sides of the Atlantic have raised concerns about privacy as it relates to IPv6 implementation.

IPv6 provides a near-limitless number of Web addresses. The change from 32-bit IP addresses to 128-bit IP addresses is allowing the Internet—and internal networks—to be used in ways not previously possible.<sup>1</sup>

One of the primary benefits of the Internet—the ability to transmit huge amounts of data instantaneously around the world—is also its major weakness when it comes to data protection. Vast amounts of information about Internet users are collected each day—sometimes without their knowledge or consent. As people conduct more and more of their business online, they are leaving a larger electronic “footprint” for would-be thieves to raid. Viruses, Internet worms, spam, botnets, spoofing, and other forms of online attacks have so far proven a difficult problem to contain, and a conversion to IPv6 will introduce new privacy and security challenges.

### **What Is IPv6 and How Will it Affect Businesses?**

Internet Protocol version 6, or IPv6 for short, is the latest edition of the platform which supports the entire Internet. The current version, IPv4, has existed for 20 years and is considered by many to not have the capacity that future business will demand. Experts have been calling for a next-generation Internet Protocol since 1994.

That update is here. All U.S. federal agencies must be IPv6-compliant by mid-2008. Given the number of companies that do business with the U.S. government, the federal mandate should lead to accelerated conversions in the commercial realm as well.

As far as businesses are concerned, one of the greatest promises of IPv6 is the new platform’s ability to provide a nearly limitless supply of Internet addresses. It’s already in most of our routers, switches, and new phones and operating systems.

To put things in perspective, IPv4 supports around 4.2 billion distinct Internet addresses—or fewer than one for every person on the planet. IPv6, on the other hand, supports 340 undecillion (one undecillion has 36 zeroes) addresses. That is more than enough so that IP addresses will never be a scarce resource again.

IPv6 is emerging at the same time as wireless broadband networks that necessitate an increase in IP addresses and greatly expand the practical applications for those IP addresses. This new source of Internet addresses will enable an entire new generation of complex wireless devices, for example.

The possibilities and potential benefits of IPv6 are particularly staggering in the supply chain industry. Every package, parcel, and cargo crate could have its own unique Internet address, and wireless broadband technology will allow that address to be transmitted cheaply and easily. So customers and shipping companies will be able to go online and instantly track their package to a precise location anywhere in the world, in much the same way as GPS systems currently track vehicles on the highways. Through IPv6, these items can have their own routable Internet addresses without the need for any Internet server. This technology can vastly improve how companies track and ship cargo, providing both cost savings for companies and better service for customers.

IPv6 also has significant implications for the personal safety and homeland security industries. Specific information—a crash victim’s medical records, for example—can be automatically collected and sent to the appropriate authorities using this new technology, similar to the way packages can be tracked in shipping.

First responders, such as fire fighters and police departments, have faster and more reliable electronic communications with each other utilizing an IPv6 platform rather than an IPv4 platform. This is due to the “end-to-end” communications features of IPv6 that are not available in IPv4. For example, cities across America are implementing municipal-wide IPv6 wireless networks that substantially aid first responders in that community.

Some have speculated that an organization can obtain lower charges from its Internet Service Provider (ISP) because IPv6 will enable the organization to purchase fewer public Internet addresses from the ISP and instead use the additional addressing features of IPv6 to enable Internet communications to and from PCs on the organization’s internal network.

The U.S. government has set a June 30, 2008 deadline for all government agencies to be IPv6-compliant.<sup>2</sup> However, most agencies are not on track to meet that deadline. To date, the nation lacks a single, organized effort to implement IPv6. A significant step towards expanding IPv6 compliance in the United States is Microsoft’s decision to make its newest version of the Windows operating system IPv6-compliant.

### **The Slow Start to IPv6 Implementation**

In the United States, the federal government is a leader in conversion to IPv6. Many expect the private sector will follow the government’s lead, particularly as companies that contract with federal agencies need to become IPv6 compliant.

But so far, the switch from IPv4 to IPv6 has started slower than originally anticipated. That makes it more difficult to assess the privacy and data security ramifications, since the new Internet platform isn’t being employed in enough real-world situations.

A 2006 report by the Government Accountability Office (GAO) (*see References section at the end of this ar-*

<sup>1</sup> <http://www.commandinformation.com/ipv6/anatomy/>

<sup>2</sup> <http://www.commandinformation.com/federal/OMB522/>

title) found that federal agencies have taken some steps in planning for IPv6 conversion, but several agencies have not completed important parts of the process. Many Asian nations, particularly China and Japan, have been far more aggressive in pushing along IPv6.

Ten of the 24 major agencies surveyed by the GAO still had not developed IPv6-related policies and enforcement mechanisms at the time of the report. The report's authors found that many agencies had not yet prepared to capitalize on the advantages of IPv6, largely because they lacked incentives to use IPv6 or because they weren't far enough along in the transition process. And while 23 of the 24 agencies had at least begun an impact analysis of IPv6, only nine had assessed the costs associated with IPv6 conversion. As of 2007, approximately 70 percent of federal agencies are on track to compliance.

The federal government has set clear and laudable goals for IPv6 implementation, but so far, actual conversion from IPv4 to IPv6 has fallen far short of those goals. While experts may speculate, the true data security and privacy strengths and weaknesses of IPv6 won't fully be known until after the new platform is in widespread, day-to-day use throughout the world.

### How Does IPv6 Affect the Privacy and Data Protection Landscape?

The uncertainties of IPv6 create security concerns for companies and individuals. The ability to collect and transmit massive amounts of data instantaneously is a blessing and a curse: while this capacity has revolutionized how business is transacted, it also has put confidential customer and employee information at risk as never before. The broader the access, the greater the risk, and IPv6 carries with it no small amount of concerns in that regard. Personal data processing systems that do not meet the European Commission's Directive on Data Protection (ECDDP) threaten to impede the flow of information between EU and U.S. organizations.<sup>3</sup>

With its potential for "stateless" autoconfiguration of unique IP addresses, IPv6 can expose users to a greater privacy risk. This autoconfiguration technology opens up the potential to track the same unique identifying number embedded in an IPv6 address each time a user obtains or exchanges information over the Internet. The first 64 bits of an IPv6 address describe the network and can change across connections to different networks, but the second 64 bits of the IP address are the "Interface Identifier," which stays the same in autoconfiguration for a particular device or host. Some have called this globally unique Interface Identifier "a second Social Security number."

In contrast, consumers' IPv4 addresses are only 32 bits total and often do not have an embedded number that is constant and unique due to IPv4 technologies like Network Address Translation and Dynamic Host Configuration Protocol that result in periodically or frequently changing the IP addresses assigned to a particular PC. Organizations that collect the IP addresses of consumers may need to review their privacy notices regarding the collection of a globally constant and unique number in IP addresses of IPv6 users. If an IPv6 laptop is autoconfigured to have a globally constant In-

terface Identifier in the IP address, then geo-privacy issues are raised when the laptop is used in different locations, say, on a business trip. The same Interface Identifier address can be tracked every time the traveler uses her laptop in different locations. There are optional "fixes" for the IPv6 autoconfiguration privacy issues. Through a privacy-enhancing technology adoption, instead of a unique, unchanging identifying number, each user can receive a periodically changing pseudo-random number.

The improved Internet platform also can be used to provide better protection for online users. The European Commission's IPv6 Task Force to the Data Protection Working Group calls IPv6 a "potentially powerful tool to improve the possibilities of user privacy."

Built-in security and privacy features of IPv6 provide protections for users that do not exist in most implementations of the current Internet protocol. However, those features must be supported with the user's own data security efforts to be truly effective.

Another security challenge is political, not technical. Governments and law enforcement agencies continue to push for greater access to personal information as part of the global war on terror. As IPv6 expands the Internet into new areas of communications, it stands to reason that law enforcement may seek greater oversight with respect to these areas, too. One commentator has recommended transition in public and private networks to IPv6 to improve tracking and tracing of IP communications for counter-terrorism purposes (see *Westby article cited in References at the end of this article*). Law enforcement will still need to grapple with the fact that IPv6 supports an optional "privacy extension" that can be used to change the Interface Identifier with every different connection to the Internet, making it harder for law enforcement to trace Internet activity to a particular PC or person.

### Measures to Improve Online Security in IPv6

One major positive step is that Internet Protocol security (IPSec) is mandatory with IPv6, while it is only optional in IPv4. IPSec is a set of protocols designed to make sure that information "packets" are securely exchanged between computers at the IP level. It provides the user with some protection against data theft, hacker attacks, and user credential theft.

Also, while no one body has full control of IPv6 implementation, many of the major parties involved at least realize that privacy and data protection are real and urgent considerations.

The European Commission wrote in 2002, "Due to the fact that the Internet has, from the very beginning, been considered as an open network, there are many characteristics of its communication protocols, which, more by accident than design, can lead to an invasion of privacy of the Internet users . . . . It is therefore indispensable that the European Commission and the European Union as a whole consider privacy issues in the further development of the Internet." (See *cite in References section at the end of this article*.)

The International Working Group on Data Protection in Telecommunications published a ten-point overview plan back in 1996, although the recommendations remain valid today. The group's recommendations have not and probably will not be adopted on any type of worldwide basis, but they represent a consensus of IPv6 experts and, as such, their recommendations should

<sup>3</sup> Mapping Security pg. 122, Tom Patterson

### IPv6 Issues for Privacy Lawyers

Here is a short list of legal issues of interest to privacy lawyers regarding IPv6. With a technology as new and transformational as IPv6, there are, of course, many other issues, including issues yet to be identified.

1. If you are a federal government employee, ask appropriate persons how your agency is doing in moving to IPv6 compliance by the June 30, 2008 deadline and how the transition affects you as an information user in the agency. Stated differently, are we getting our own house in order?

2. Be aware that IPv6 may have important implications for computer forensics and the admissibility of evidence. For example, IPv6 traffic with its mandatory IPSec security feature may, in some cases, make it easier to prove that a particular computer or Internet activity was performed on a unique PC or by a particular person. IPSec includes technology to authenticate the source or recipient of a communication, which is also sometimes referred to as “non-repudiation”—proving a communication was sent or received by a particular person.

3. The autoconfiguration feature of IPv6 uses an algorithm applied to a 48-bit “MAC” address unique to every computer or device. This is done to provide the 64-bit unique “Interface Identifier” that is part of the IPv6 address. The 48-bit number MAC address is encoded in the “Network Interface Card” of the computer by the manufacturer. It is conceivable that evidentiary issues may arise where it is claimed that someone had physical access to a computer and swapped Network Interface Cards to attempt to link computer activity to a different person, or even that a different 48-bit MAC address was loaded into the autoconfiguration algorithm without physical access to the Network Interface Card. The result would be a unique Interface Identifier being associated with a PC or person not actually involved with the activity.

4. In nations that regulate the retention period of certain types of personal data, in some circumstances an IPv6 address with a unique Interface Identifier that can be associated with a particular individual may be personal data that may need to be deleted after a transaction is completed.

5. It will be interesting to see if case law develops that in particular types of network and telecommunications implementations, the standard of care dictates that IPv6 rather than IPv4 be implemented due to the additional security features of IPv6, including mandatory IPSec as described above. Applicable standards of care can require that new technologies be implemented even where the technologies are not generally implemented by similarly situated entities. See, e.g., *The T.J. Hooper*, 60 F.2d 737 (2d Cir. 1932), cert. denied, 287 U.S. 662 (1932) (opinion by Honorable Learned Hand; barge was negligent for not having a weather warning radio even though the vast majority of similar barges did not have such a radio).

6. The extra-territorial jurisdiction of nations to regulate data processing occurring outside their borders about their citizens is an issue that will continue to evolve and present unique challenges. The unique auto-configured Interface Identifier in IPv6 traffic may result in a nation seeking to extend its extra-territorial reach to foreign data processors collecting personal data about citizens of such nation.

carry a great deal of weight during IPv6 implementation. The Group’s ten points are as follows:

1. Service providers should inform each potential user of the Internet unequivocally about the risks to her privacy. She will then have to balance these risks against the expected benefits.

2. In many instances the decision to enter the Internet and how to use it is subject to legal conditions under national data protection law.

3. Initiatives to arrive at closer international cooperation, even an international convention governing data protection in the context of trans-border networks and services, are to be supported.

4. An international oversight mechanism should be established which could build on the existing structures such as the Internet Society and other bodies. Responsibility for privacy protection will have to be institutionalized to a certain extent.

5. National and international law should state unequivocally that the process of communicating (e.g. via electronic mail) is also protected by the secrecy of telecommunications and correspondence.

6. Furthermore, it is necessary to develop technical means to improve the user’s privacy on the Internet. It is mandatory to develop design principles for information and communications technology and multimedia hard and software, which will enable the individual user to control and give him feedback with regard to his personal data. In general, users should have the opportu-

nity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service.

7. Technical means should also be used for the purpose of protecting confidentiality. The use of secure encryption methods must become and remain a legitimate option for any user of the Internet. The Working Group supports new developments of the Internet Protocol (IPv6), which offer means to improve confidentiality by encryption, classification of messages and better authentication procedures. The software manufacturers should implement the new Internet Protocol security standard in their products, and providers should support the use of these products as quickly as possible.

8. The Working Group would endorse a study of the feasibility to set up a new procedure of certification using “quality stamps” for providers and products as to their privacy-friendliness. This could lead to an improved transparency for users of the Information Superhighway.

9. Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society without questioning the principle as such.

10. Finally, it will be decisive to find out how self-regulation by way of an expanded “Netiquette” and privacy-friendly technology might improve the implementation of national and international regulations on

privacy protection. It will not suffice to rely on any one of these courses of action: they will have to be combined effectively to arrive at a Global Information Infrastructure that respects the human rights to privacy and to unobserved communications.

You may ask, that is all fine, but what should my organization be doing to address IPv6 privacy and security issues? Here is a starter list:

1. Understand the new technology capabilities of IPv6 and make a business decision about whether, when and how your organization will implement IPv6 or become IPv6-ready. The European Union is aggressively supporting IPv6 to achieve a global competitive advantage.

2. Understand the security-enhancing features of IPv6 as well as the features of IPv6 that raise new security challenges. Design and build IPv6 security in your network from the beginning—you have a fresh start (as opposed to the current environment of 20 years of IPv4 security patches and add-ons).

3. Understand and address the security challenges in transitioning from IPv4 to IPv6. Even if you move your entire organization to IPv6, your trading partners and the rest of the world will not all move to IPv6 in sync with your organization. IPv6 clients (e.g. PCs) in your organization will still need to communicate with the outside world.

4. Understand and address the security threats to your organization's IPv4 network devices (e.g., firewalls, routers, etc.) and clients from incoming IPv6 traffic that exists today. Even if you decide you do not need to transition your systems to IPv6 in the foreseeable future, hackers are already using IPv6 technologies to attack IPv4 systems. For example, unless a system administrator implements proper protective controls, an attacker may be able to send IPv6 malicious code through an IPv4 "tunnel" and install backdoor programs on an IPv4 host or client that do no show up in IPv4 security scans. Also, IPv4 firewalls may need to be specifically configured to recognize and filter IPv6 traffic.

5. Make sure you identify IPv6 clients that may be accessing your network without your knowledge. For example, an employee may connect a personal Windows Vista™ PC to your network. Windows Vista™ ships with IPv6 "default on." Through IPv6, the Vista™ PC could be telling outsiders its site-local address within your network, exposing the PC to new threats by attackers. Also, PC users can easily self-install IPv6 in Windows XP PCs, and in some network configurations the network administrator will not be able to detect the IPv6 installation.

6. Incorporate IPv6 security risk management into your supply chain processes. Do this for technology acquisitions and also regarding vendors and business partners who have access to sensitive organization information, including trade secrets and sensitive personally identifiable information. Just as your own organization needs to manage IPv6 security challenges in its own systems, your organization should address how its vendors are addressing IPv6 in their systems.

7. IPv6 calls for a fundamental re-evaluation of basic information security models. In IPv4 networks, the "perimeter defense" concept prevails; this means there are protective firewalls, gateway routers, internal routers, and other devices that stand between the Internet and the network's hosts and clients (e.g., PCs). In contrast, the "plug-n-play" nature of some IPv6 implementations

can mean there is a "virtual" network that is distributed beyond an organization's "perimeter." There is no perimeter firewall—distributed devices each have their own firewalls. In short, if you proactively address IPv6 security, you can get more security for a lot less money. Conversely, if you ignore the security changes that come with IPv6, you'll end up with a lot less security for a lot more money.

## IPv6 Issues for Privacy Lawyers

Here is a short list of legal issues of interest to privacy lawyers regarding IPv6. With a technology as new and transformational as IPv6, there are, of course, many other issues, including issues yet to be identified.

1. If you are federal government employees, ask appropriate persons how your agency is doing in moving to IPv6 compliance by the June 30, 2008 deadline and how the transition affects you as an information user in the agency. Stated differently, are we getting our own house in order?

2. Be aware that IPv6 may have important implications for computer forensics and the admissibility of evidence. For example, IPv6 traffic with its mandatory IPSec security feature may, in some cases, make it easier to prove that a particular computer or Internet activity was performed on a unique PC or by a particular person. IPSec includes technology to authenticate the source or recipient of a communication, which is also sometimes referred to as "non-repudiation"—proving a communication was sent or received by a particular person.

3. The autoconfiguration feature of IPv6 uses an algorithm applied to a 48-bit "MAC" address unique to every computer or device. This is done to provide the 64-bit unique "Interface Identifier" that is part of the IPv6 address. The 48-bit number MAC address is encoded in the "Network Interface Card" of the computer by the manufacturer. It is conceivable that evidentiary issues may arise where it is claimed that someone had physical access to a computer and swapped Network Interface Cards to attempt to link computer activity to a different person, or even that a different 48-bit MAC address was loaded into the autoconfiguration algorithm without physical access to the Network Interface Card. The result would be a unique Interface Identifier being associated with a PC or person not actually involved with the activity.

4. In nations that regulate the retention period of certain types of personal data, in some circumstances an IPv6 address with a unique Interface Identifier that can be associated with a particular individual may be personal data that may need to be deleted after a transaction is completed.

5. It will be interesting to see if case law develops that in particular types of network and telecommunications implementations, the standard of care dictates that IPv6 rather than IPv4 be implemented due to the additional security features of IPv6, including mandatory IPSec as described above. Applicable standards of care can require that new technologies be implemented even where the technologies are not generally implemented by similarly situated entities. See, e.g., *The T.J. Hooper*, 60 F.2d 737 (2d Cir. 1932), cert. denied, 287 U.S. 662 (1932) (opinion by Honorable Learned Hand; barge was negligent for not having a weather warning radio even though the vast majority of similar barges did not have such a radio).

6. The extra-territorial jurisdiction of nations to regulate data processing occurring outside their borders about their citizens is an issue that will continue to evolve and present unique challenges. The unique auto-configured Interface Identifier in IPv6 traffic may result in a nation seeking to extend its extra-territorial reach to foreign data processors collecting personal data about citizens of such nation.

### Summary

IPv6 should not be considered a “magic bullet” for user privacy any more than it should be looked upon as a step backward for data protection. Instead, IPv6, like the current Internet protocol, provides both opportunities and challenges for information privacy and protections. The onus ultimately will remain on administrators and users of IPv6 technology to ensure that their employee, customer and client data is stored and transmitted securely.

### REFERENCES

(All sites last visited on Aug. 9, 2007)

Comments before the National Institute of Standards and Technology (March 8, 2004), available at [http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/comments/EPIC\\_IPv6.htm](http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/comments/EPIC_IPv6.htm)

Communication from the Commission to the Council and the European Parliament, *Next Generation Internet-Priorities for Action in Migrating to the New Internet Protocol IPv6* (2002), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002DC0096:EN:HTML>

Convery, Sean and Miller, Darrin. *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v*

*1.0)*, 2004, available at [http://www.cisco.com/web/about/security/security\\_services/ciag/documents/v6-v4-threats.pdf](http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf)

Davies, Joseph. *IPv6 Improvements in Windows Vista*, 6Sense Newsletter (2006), <http://www.usipv6.com/6sense/2006/apr/01.htm>

Government Accountability Office, *Internet Protocol Version 6: Federal Government in Early Stages of Transition and Key Challenges Remain* (June, 2006), available at <http://www.gao.gov/new.items/d06675.pdf>

International Working Group on Data Protection in Telecommunications, *Draft Report and Guidance on Data Protection on the Internet*, (May, 1996), available at [http://trout.cpsr.org/cpsr/lists/rre/Data\\_Protection\\_and\\_Privacy\\_on](http://trout.cpsr.org/cpsr/lists/rre/Data_Protection_and_Privacy_on)

Kaisor, Basar et al., *IPv6: Legal Aspects of the New Internet Protocol* (Euro6IX, 2005), available at <http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf>

Marsan, Carolyn Duffy. *Windows Vista Not Playing Well with IPv6*, PCWorld (2007), available at <http://www.pcworld.com/article/id,132689-c,vistalonghorn/article.html>

National Telecommunications and Information Administration, *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)*, (January 2006), available at <http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/ipv6final.pdf>

Westby, Jody R., *Countering Terrorism with Cyber Security*, (August 2006) p. 14, available at <http://www.cyberconflict.org/pdf/JodyWestby-WFS-TerrorismFlourishesPaperv6.pdf>

Warfield, Michael H. *Security Implications of IPv6*, Internet Security Systems 2003 available at <http://documents.iss.net/whitepapers/IPv6.pdf>



