Tracking Down Anonymous Internet Abusers: Who Is John Doe?

Raymond Placid, Florida Gulf Coast University
Judy L. Wynekoop
Tracking Down Anonymous Internet Abusers: Who Is John Doe?

In the past 10 years, Internet usage in the United States has doubled, with nearly 239 million Americans logging on. This growth has led to a proliferation of legal infringements such as identity theft, copyright violations, and defamation by anonymous bloggers. As Internet usage continues to grow, so too, will the demand for the legal profession to redress these infringements. Unfortunately for the legal profession, the Internet generates a new type of defendant. We shall call this defendant “John Doe.”

Who is John Doe?
John Doe is the person who blogs anonymously on the Internet and infringes upon your client’s legal rights. John Doe does not have to be a sophisticated blogger to remain anonymous because the technology that drives the Internet has evolved without accountability. Blogging from a hotspot or through a proxy server can obscure the true identity of the blogger. The mere delay in attempting to track down an anonymous blogger can lead to anonymity because the address logs may have been overwritten by the Internet service provider.

Tracking down Internet abuse can be challenging from a legal and technological perspective. For example, if a person has been defamed anonymously on a website, the website is not likely to release the name of the anonymous blogger without a court order. The costs of taking legal action to obtain a court order can be taxing from both an economic and personal perspective, and in some cases will serve as a roadblock for the injured party. Assuming that the court grants the injured party an order to obtain the data from the website, there is a good chance that the anonymous blogger’s website registration data will be fictitious. Many bloggers do not provide accurate registration data to a website. Even the email address given to a website by the blogger could be fictitious because email addresses can be easily obtained using false registration data.

This article will address some of the more common technological roadblocks (i.e., the IP address, hotspots, and proxy servers) that an attorney can run into when attempting to track down anonymous Internet abusers. We will begin our discussion with the IP address system.

The IP Address System

The IP address system allows computers to recognize one another and transfer data over the Internet. The original IP address system is referred to as Internet Protocol version 4 or IPv4. IPv4 can generate approximately 4.3 billion IP addresses. In 1995, Internet Protocol version six, or IPv6, was developed to accommodate the growth of the Internet. IPv6 can generate over 340 undecillion IP addresses. Both systems, IPv4 and IPv6, are still in use today, although it is expected that the IPv4 address system will be exhausted within the next few years.

As private computer networks developed and Internet usage grew, the IP address system began to use temporary address assignments. When the computer’s IP address is temporary, it is referred to as dynamic. In contrast, when a computer is configured to use a permanent IP address, it is known as a static IP address. It should be noted that although residential customers are generally assigned dynamic IP addresses, in actuality, they change infrequently.

Theoretically, it should be very easy to track down the IP address of an anonymous blogger because the address should be stored in IP address logs. For example, as an anonymous blogger logs on to the Internet, his computer will be assigned an IP address by the Internet service provider (e.g., AT&T, Comcast, etc.). The IP address assignment will be stored in a log that is maintained by the Internet service provider. This IP address will generally be attached to data that is sent from the anonymous blogger’s computer to its destination (e.g., web server). If the IP address of the blogger is obtained from the destination web server, then the address can be traced back to the Internet service provider. The Internet service provider’s logs should identify which customer was using that IP address. From there, the IP address can be traced to the customer’s computer, and ultimately the anonymous blogger can be identified.

The reality is that tracking down the IP addresses of an anonymous blogger can be very difficult because IP address logs are periodically purged. Therefore, if the IP address information is not sought in a timely manner, the anonymous blogger’s trail will be erased.

The matter is exacerbated if the anonymous blogger logs on to the Internet from a business because there may be two IP addresses to track down: 1) the IP address assigned to
wireless Internet access. These are generally referred to as “hotspots.” In a typical hotspot environment, there are two addresses that are utilized to transfer data over the Internet: 1) the hotspot’s IP address and 2) the MAC address of the patron’s laptop computer network card. A MAC address is a unique number that is assigned to a network card (wireless or otherwise) by the manufacturer and allows a computer to be uniquely identified on a local network. The hotspot’s network hardware will use the MAC address to communicate with the patron’s laptop. The hotspot’s network hardware will attach its IP address to the patron’s data to transfer it over the Internet. The MAC address of the patron’s network card will never be transmitted beyond the hotspot’s router, but it should be stored in the hotspot’s router logs. Unfortunately, hotspot router logs are generally not very large. If there is a lot of Internet traffic at the hotspot, which is typical, the patron’s MAC address will be overwritten, and they will remain anonymous.

In addition, there are several techniques that can be used to log anonymously from a hotspot. A blogger could purchase a wireless network card with cash and use fictitious data to register the card. By turning off the laptop’s wi-fi switch and using the new anonymous wireless card, the blogger can cheaply cloak his or her identity. In addition, a blogger can achieve an anonymous MAC address without purchasing anything and with minimal computer knowledge by a process known as MAC spoofing. Although the permanent MAC address of the network card cannot be changed, a user can tell the computer operating system that it is something different. This can be done by changing the properties of the network connection and manually entering any MAC address or by using third-party software. (MAC spoofing can also be used when blogging from home, and, in some instances, from work or a public access terminal.)

Proxy Servers
Finally, a blogger could use a proxy server to further conceal identity. Proxy servers are Internet services that allow bloggers to hide their IP addresses. If a blogger uses a proxy server, the proxy server re-packages the message using its own IP address as the sending address. As the destination website receives the message, the transmission appears to have originated from a proxy server. Thus, the anonymous blogger’s IP address is not used to transmit the defamatory material to the website.

Proxy servers can be fairly complex and require software to be downloaded and configured on the user’s computer. It is possible that the anonymous blogger’s message may pass through several different proxy servers before arriving at its destination. This is sometimes called onion routing (the most popular is a service called Tor). The destination website never sees the anonymous blogger’s IP address, nor does it know the original proxy server’s IP address. The message appears to have originated at the last proxy server.

No matter how many proxy servers are involved in transmitting a message through the Internet, the protocols remain the same. Data cannot be transferred from an anonymous blogger’s computer without an address. If the anonymous blogger accesses a proxy server before sending defamatory material to the destination website, there is still a trail, the IP addresses. Even if the IP address is disguised, it may be traceable if the proxy server preserves the IP address logs that are created to associate the sending computer’s IP address with a particular communication. Unfortunately, proxy servers have no incentive to maintain IP address logs because their systems are designed to preserve anonymity. As a consequence, it will be very difficult to track down an anonymous blogger that travels through cyberspace via proxy servers, because the IP address logs will almost certainly be intentionally erased by the time they are subject to discovery.

There are other methods of maintaining anonymous communications. These methods include encryption, scrambling the order of packets, and mixing the actual packets from multiple messages with fake packets. These methods are beyond the scope of
this article because they require some degree of technical sophistication and are not common blogging techniques.

Tracking Issues and Strategies

The ability to track down the anonymous blogger should be one of the primary issues that should be considered by counsel in deciding whether to pursue an action against John Doe. There are two sides to this issue — legal and technical. The substantive legal issues will not be addressed in this article, but attorneys faced with anonymous bloggers should be aware that some Internet service providers are notorious for challenging the right of the plaintiff to discover confidential data. If the website challenges the disclosure of registration or IP address data on legal grounds (e.g., privacy rights, constitutional, etc.), accelerated discovery techniques and in-camera inspections should be employed so as to preserve the data. As part of the discovery requests, both website registration data and IP address information should be requested. If the registration data is fictitious, then IP address tracking will be required. There are several Internet services that can be utilized to assist an attorney with tracking IP address data.

If IP address tracking is required, the address will lead to one of two places: a proxy server or an Internet service provider. If the IP address leads to a proxy server, the chances of tracking down John Doe are low. If the IP address leads to an Internet service provider, additional discovery will be needed to obtain the registration data and IP address logs from the provider. The information from the Internet service provider will generally lead to one of three places: a home computer, a business, or a hotspot. If the Internet service provider's data leads to a home computer, there is a good chance that counsel will be able to identify the owner of the computer because IP address allocation from Internet service providers to home computers changes infrequently. On the other hand, if the IP address leads to a business or hotspot, still additional discovery will be required. For a business computer network, the discovery should focus on the internal (i.e., private) IP address logs. For a hotspot, the discovery should focus on the MAC address. Identifying John Doe will be much more difficult in a hotspot environment because the router logs are frequently overwritten. As an example, Osama Bin Laden's couriers successfully used hotspots to transmit data over the Internet in order to cloak their identity.14

The key thing to remember is that time is of the essence. One of the primary reasons that bloggers remain anonymous is that their trails fade away with time. IP address logs are purged periodically by service managers (e.g., business organizations, proxy servers, hotspots) as part of routine maintenance, and currently there are no regulations or standards in the industry requiring IP address logs to be preserved for a minimum time period. As a consequence, an attorney's discovery techniques must be designed to move quickly through the legal system in order to identify an anonymous blogger.

Conclusion

An attorney can run into many obstacles in attempting to track down Internet abusers. The first obstacle may be the legal system itself. It is unlikely that a website will release the personal data of the Internet abuser without a court order. This can become a fairly time-consuming process because some website owners will challenge the right of the plaintiff to obtain the information concerning the anonymous blogger based on constitutional and privacy concerns. The longer it takes to track down an Internet abuser, the more likely the trial (i.e., the IP address) will be erased.

In addition, the technology that drives the Internet has evolved without accountability. As a consequence, it takes very little effort or sophistication to remain anonymous on the Internet. If John Doe enters the Internet through a wireless hotspot, there is a good chance that he or she will remain anonymous because the hotspot's router logs will probably be overwritten by the time you reach them. If John Doe surfs the Internet through an elite proxy server, there is an even stronger chance that he or she will remain anonymous because proxy servers are designed to obscure the blogger's footprint.

At the end of the day, the attorney may discover this much about John Doe: His IP address was 172.0.6.223.121; his name remains a mystery.15

2 See Melvin v. Doe, 836 A.2d 42, 50 (Pa. 2003), where a judge unsuccessfully sued an anonymous blogger for defamation. After several years of pursuing the defendant, the judge was unable to discover the identity of John Doe through the legal system.
4 Id.
5 Id.
7 American Registry for Internet Numbers, IPv4 depletion, IPv6 Adoption, (Feb. 3, 2011).
9 Id.
12 See Barath Raghavan, Tadayoshi Kohno, Alex C. Snoeren & David Wetherall, Enlisting ISPs to Improve Online Privacy: IP Address Mixing by Default, PRIVACY ENHANCING TECHNOLOGIES 143 (2009).

Raymond L. Placid is an associate professor at the Florida Gulf Coast University in Ft. Myers, where he teaches business law and other related courses.

Judy Wynekoop is the associate dean for the Leitigert College of Business at Florida Gulf Coast University, where she is also a professor of computer information systems.

This column is submitted on behalf of the Trial Lawyers Section. Craig Anthony Gibbs, chair, and D. Matthew Allen, editor.