The Electronic Frontier Foundation

User Privacy for ISPs and Accidental ISPs.

The Digital Millennium Copyright Act gives people who claim to own copyrights tremendous power to invade the privacy of Internet users. With only a clerk's stamp on a form, almost anyone can demand that an Internet service provider reveal its users' personal information – if the ISP has that information. If you're served with a subpoena, as the RIAA showed Verizon in court, you don't get to choose whether or not to respond. This means your data is at the mercy of not just record companies seeking out music swappers, but also private detectives, spammers, and cranks of all kinds who might demand users' names and addresses.[1] Whether you're a big ISP or dorm-room sysadmin, you can preserve your users' privacy best by not keeping any logs containing that information or connecting them to online activity in the first place – you can't be made to disclose information you don't have.

If you are not in business as an ISP, but are providing network connectivity – for example, offering wired or wireless access to library patrons, visitors at a café, or friends and neighbors in a residence – you may still be the target of one of these information demands. But as a non-commercial ISP, you've probably got no good reason to keep this info in the first place. In fact, you may want to become an "accidental ISP" in order to provide some additional privacy for people downstream from your router. Changing the way that you keep records and connect your users in simple ways can help you limit the legal hassles you'll face as a non-commercial ISP.

Computers are uniquely identified on their networks by IP address.[2] To protect privacy, network administrators can opt to assign pools of IP addresses dynamically, rotating a fixed number of addresses randomly among a group of users, then delete assignment logs promptly to protect the privacy of users. EFF is not aware of any law that requires ISPs to keep any records that would tie particular IP addresses to particular user identities.

Privacy-enhancing network management.

Many networking tools – from your DHCP server to your webserver – can be configured to capture a little or a lot of information about your users. Start by configuring these tools to log only the information you need for troubleshooting and network security, and by flushing your logs after you're done with them.

---

[1] In *RIAA v. Verizon*, the recording industry forced Verizon to disclose the names and addresses of subscribers accused of sharing files using KaZaA. EFF and 44 other consumer privacy groups and ISPs filed a brief in that case to protest the broad user privacy implications. Because the law does not look into the basis for the copyright complaint before demanding compliance with the subpoena, but relies on the requester's "good faith," it is ripe for abuse by stalkers, identity thieves, and criminals. All that someone needs to start is an IP address, which can be picked out of any email, instant message, or download obtained from a file-sharing network.

[2] Internet Protocol (IP) addresses may be private to a local-area network (often gated to the Internet via NAT) or routable on the Internet. DHCP can be used with either type of address.

Even though hard drives are cheap, there are hidden costs to packratting data about your users, like the expense of keeping that information away from legal attackers who use bad laws to undermine the privacy citizens of a free society need. Think twice before you capture data, and think three times before you store it.

Purge data logs you don't need. Set a regular schedule to erase logs and backups you no longer need, using strong deletion utilities.[3] If you reuse media, do a strong delete before rewriting. Overwrite free space and swap files so you're not inadvertently retaining data.

Scrub the logs you do need to remove extraneous information, particularly personally identifiable information. For example, if you're interested in what country your users are coming from, resolve IP addresses to a national origin and then flush the IPs themselves.

If you don't need information on who's connecting when (and you usually don't), here are some concrete ways to structure your network to enhance privacy:

- Assign dynamic IP addresses and don't keep logs of past assignments. Once a DHCP lease ends, flush it from the logs.
- Turn down DHCP lease time.
- If you authenticate users by MAC addresses, don't keep records of who uses which MAC.
- If you connect dial-up users, don't log the caller ID and user ID to IP address pairings.

Becoming an "accidental ISP" to protect privacy.

Inexpensive networking equipment is putting an increasing number of people in the role of network administrators. For example, for less than $100, one user in a college dorm can run an open Wi-Fi router to provide wireless network access to an entire floor. Properly configured software on the wireless router can make the identities of individual users difficult to ascertain. If your service provider's terms permit it, you may want to set up such a network.

For more information, please visit the EFF website, <http://www.eff.org/>

[3] Simply deleting data from a hard drive, or even writing over it, doesn't remove all its traces from the media. Undelete utilities and forensic analysis can often recover data that has been only weakly deleted. Strong deletion utilities (also known as secure deletion utilities) write over the old data enough times to clear those remnants.