ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

The Computer Fraud and Abuse Act Must Allow for Anonymity and Privacy to Protect the Security of Ordinary Users and Promote Human Rights Around the Globe

The Computer Fraud and Abuse Act's vague and overly broad provisions threaten efforts by users to protect their privacy and security.

Often computer users wish to conceal their identifying information to protect themselves from identity theft, to speak out on controversial issues, or simply to keep their personal lives from prying eyes. Allowing people to participate in public debate anonymously has long been a part of the American tradition, since the Federalist Papers.

Anonymity is important on the global stage, too. Activists who are speaking out against oppressive regimes face serious threats of reprisals, and need to protect their identities online to ensure their physical safety, even when using communications systems based in the U.S. and so subject to U.S. law.

- **Terms of Service Violations Should Not Be a Federal Crime**. Users may try to protect their identities by simply providing a different age, using a pen name for online posts, or listing a mailbox service instead of their home address. But taking these privacy-protective steps may violate the service's fine print. Taking measures to protect privacy that happen to violate a website's terms of service should not be a crime.

- **Clearing Cookies Should Not Be a Federal Crime**. Some Internet websites store information meant to restrict a user's access to the site on a "cookie," which is a small file stored on the end-users computer. Since cookies can be used to track the user's movements from website to website, many privacy and security experts recommend that users regularly clear them. Clearing cookies should not be a crime—for people trying to protect their privacy, this is normal, everyday behavior.

- **Changing Technical Identifiers Should Not Be a Federal Crime.** There are many reasons why a user might access a site after changing technical identifiers like Internet Protocol (IP) addresses or Media Access Control (MAC) addresses.[1] For some users, it's just happenstance – if you access a website from a wi-fi café, then walk across the street and visit the same site using the public library's wi-fi, you will have a different IP address. For others, it's part of a deliberate security measure to make it harder for others to track their location or identity. For example, activists focusing on Iran and often use Tor, a software program that disguises their IP address and help shield the activists from the Iranian regime.

The CFAA's purpose was to promote computer security against criminals seeking unlawful access to do real harm. Its language must be updated to ensure that it does not turn users' measures to protect their own privacy and security into crimes.

[1] An IP address is a unique number assigned to a computer or a router when it is connected to the Internet, like how a street address identifies a particular building. A MAC address is a number that uniquely identifies a piece of computer hardware, like a serial number does.