# The Password Protection Act of 2012

## HOW IT WORKS

The Password Protection Act would make it illegal for an employer to compel or coerce access to any online information stored anywhere on the Internet if that information is secured against general public access by the user.

This is accomplished by prohibiting employers from compelling or coercing access to, and subsequently retrieving information from, *the online servers where private user information is stored.* (These servers are referred to as "protected computers" in the legislation.)[1] This broad approach mirrors the approach of the existing federal anti-hacking statutes and has several key benefits:

- **Builds on Existing Law.** The Password Protection Act's focus on where information is stored, rather than how it is accessed, reflects the approach of the Computer Fraud and Abuse Act, the federal government's primary anti-hacking tool.

    - This tool has been used for years by federal prosecutors and private individuals and companies to protect the integrity of internet systems against hackers, including protecting online email accounts[2] and Facebook accounts[3] against the stealing of passwords.

- **Technology-Neutral.** By focusing on the servers where information is ultimately stored, the Password Protection Act avoids the tricky business of identifying and defining particular types of internet services (e.g., social networking websites, email accounts, networked gaming services, cloud computing services, online storage lockers, etc.).

- **Designed to Adapt to New Internet Innovations.** The Internet is constantly changing and evolving, challenging our ability to create privacy protections that can grow alongside the Internet itself. Fortunately, every innovative website, social networking, storage, or communication technology is still ultimately supported by physical computer servers. By focusing on where a person's private information is stored, instead of how it is accessed, the Password Protection Act ensures that personal, private online information will be protected the eyes of prying employers even as new online technologies emerge.

- **Protects Employer Systems, NOT Employer Actions.** The Password Protection Act preserves the rights of employers to control access to their own hardware, as well as any internet software operated on behalf of the employer for work purposes (e.g., third-party sales data software or websites that facilitate collaborative work online). *However, the Password Protection Act does not allow employers to access private employee data under any circumstances, even if the employer uses its own computers to access that data.*

---

[1] *See* 18 U.S.C. 1030(e)(2)(B) ("[T]he term 'protected computer' means a computer … which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.").

[2] *See, e.g.*, United States v. Kernell, 667 F.3d 746, 748 (6th Cir. 2012) (involving the hacking of Sarah Palin's Yahoo! email account).

[3] *See, e.g.,* Facebook v. Power Ventures, 2012 WL 542586 (N.D. Cal. Feb. 16, 2012).