Kevin Hamzaj 2687959

Cyberlaw

Module 4 assignment

1 October 2023

Every internet-connected device is given an IP address, which serves as a unique identity. They can be used to locate a user and track their online activities. The human-readable addresses of websites are their domain names. A user's browser history and the websites they visit can be tracked using them. When a user visits a website, a user's computer stores a little file called a cookie on it. A user's browser history and the websites they visit can be tracked using them. Web browsers record which websites are visited by users. Search engines and marketers are only two examples of third parties to whom this data may be disclosed. The search phrases that users input are recorded by search engines.

When you use a search engine, the search engine provider receives your search terms. When you use a social media site, you give the social media firm access to your personal data, including your name, email address, and birthdate. You give your files to the cloud storage firm when you use a cloud storage service. When you use an email service, the email service provider gets access to your emails. You give the ride-sharing firm access to your location information when you use their service.

The Third Party Doctrine's applicability is being pushed to its limit by the nature of current technology. In the setting of phone calls, when there existed a definite separation between the phone company and the phone user, the Third Party Doctrine was created. The line

between users and third-party service providers is less sharp in the internet age. The storage of user data, activity tracking, and service delivery are all handled by third-party service providers. This implies that users are providing copious amounts of information to outside parties, information that can be accessed by them without a warrant.

Information categories that need to be exempt from the Third Party Doctrine. This includes extremely private information like medical and financial data as well as correspondence between attorneys and their clients. Without a warrant, the government should be prohibited from monitoring this data. Additionally, the Third Party Doctrine shouldn't apply to data that is kept in open repositories like social media posts and emails that are delivered to a large number of people. Since the public already has access to this information, more government monitoring of it is inappropriate. The Third Party Doctrine is an antiquated principle that is inappropriate in the internet age. To safeguard user privacy and stop governmental spying without a warrant, the Third Party Doctrine should be changed.