United States v. Botwin

Michael Plasmeier

Held: The request to access data stored by a 3rd party on the behalf of a user constitutes a search under the Fourth Amendment.

1. The Fourth Amendment protects the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” Here the accessing a person’s “paper and effects” constitutes “a search,” even though those papers are stored by a third party on behalf of a user. Thus, Fourth Amendment protection is applied to a person’s “papers” no matter where they reside, or how they are accessed, unless they are made available to the world.
	1. This type of encroachment on personal “papers” enumerated in the Amendment would have been considered a search within the meaning of the Amendment at the time it was adopted. Today the term “data” is commonly used in place of “papers.”
	2. Furthermore, before computers, persons held papers including letters, calendars, and records in their homes. Starting about twenty years ago, computers became alternate ways in which to store these records. At the time records were commonly stored directly on the computer’s hard drive, located inside the home. This provided a second level of protection under the Fourth Amendment, under “homes” in addition to “papers.”
	3. If the records are protected by a password, the user’s intent is to keep that information private. Like a locked briefcase, accessing the information that is protected by a password, or otherwise marked as private, constitutes a search.
2. Recently, in order to provide additional services, persons are beginning to commonly use 3rd party services to store their “papers”. These services include webmail services such as Gmail, calendar storage and syncing services such as iCloud, and data storage and synchronization services such as Dropbox. These services provide hosting of a persons’ private data as an agent of the person. Just because these services are run by a third party does not change the privacy of the information kept on them.
	1. This case clarifies the *third-party doctrine* from Smith v. Maryland, 442 U.S. 735. It extends Fourth Amendment protection the “papers” provided by a user for storage, processing, and/or analysis to a third party.
	2. The *third-party doctrine* still applies to records generated directly by the third party while doing business. For example, transaction records from United States v. Miller 425 U.S. 435 and Smith v. Maryland, 442 U.S. 735 would still remain the property of their creators – in this case, the businesses producing those records.
3. When a person signs up for these third party services, persons expect that their data is kept private. In fact, many data providers make claims about the privacy and security of data in both their advertising and terms of service. Because of these contractually-agreed terms, a person has expects that the 3rd party will keep the data private. A person has a “reasonable expectation of privacy” as under Justice Harlan’s concurrence in Katz v. United States, 389 U. S. 347. Accessing that information constitutes a search.
4. Users may sometimes choose to make data available to select other users, or the general public. As long as users expect data to remain private to a limited set of people, they do not intend the government to access it, and the data remains protected under the Fourth Amendment. Accessing that data would constitute a search. If a user makes data public to the world, then that data loses its Fourth Amendment protection, and accessing it would not constitute a search.
5. This data is also commonly downloaded on devices located outside the home. For example, a person may access his or her data on laptops and cell phones owned by the person. It does not matter if the data is being transmitted to/from the home, or to/from a third party, or is residing on the device. It is the data that is protected, not the place or the device on which it is stored.
6. A person may access their cloud data on devices owned by others. The data remains private no matter what device it is on. It is the data that is protected, not the means with which it is accessed.
7. Botwin had stored her personal financial records on her personal computer, protected with a password, using the Quicken software package. In 2011, Botwin upgraded to the new version of Quicken which integrated with Mint.com. As part of the migration, Botwin signed up for Mint.com with a password. She shared the password with her sons and instructed them to keep it private.

This action is protected because Botwin entrusted her personal data to Mint.com. Mint.com promises that they will keep her data private – her financial data is not disclosed to other people or posted publically. Only a few members of the Mint staff can access it, and they do so under Mint’s privacy policy. Botwin intended her “papers” to remain private.

Botwin did share her password with her teenage sons. However she did this under the explicit understanding that they keep the password private. This would even apply if there was a tacit understanding that the password would not be shared.

1. When Botwin purchased her iPhone, she signed up for iCloud, a service which allows persons to synchronize their calendars between devices. iCloud also allows persons to provide access to others. Botwin used this feature to share her calendar with her son.

Botwin again entrusted a third party service provider to maintain custody of her “papers.” In addition, she made her “papers” available to a limited set of third parties – namely her son. Botwin did not intend and did not provide access to government agents, thus access by them would constitute a “search.”

1. As Botwin used the Internet, a number of sites used Google’s advertising platform. As part of the platform, Google collects information about the pages which Botwin visited. Google then used this information to build an interest profile for their Interest Based Advertisements. Botwin claimed to have enabled the “Do Not Track” header in Google Chrome.

The Interest Based Advertising platform is a business record of Google. Thus, these records are not subject to Fourth Amendment protection for Botwin. The access of these records does not constitute a search for Botwin.