When someone registers to vote, their voter registration record may be considered public record and available to a variety of individuals or groups. Voter registration records typically include personally identifying information such as home address and may also include political party affiliation and other details. All U.S. states and the District of Columbia allow some sort of access to these records, although who has access and what information is available varies across the country. Privacy protections of voter records also vary from state to state. Voter privacy is important to survivors of domestic violence, sexual assault, stalking, or trafficking who are concerned about their personal information being released or accessed by an abusive person. Many survivors have to navigate a complex and confusing system to maintain their privacy and some, unfortunately, ultimately decide not to vote at all to avoid any possibly safety risks.

**What’s Available & To Whom**

All states allow access to voter registration records for political parties and candidates for elected offices. According to the National Conference of State Legislature’s [February 2016 report on voter records and privacy](https://www.ncsl.org/research/elections-and-campaigns/voter-records-and-privacy.aspx), only eleven states do not share voter information with the general public and some states limit who can access the records. For example, access may be limited only to residents of the state, to other registered voters, to non-profit organizations, or for research purposes. Most states, however, allow public access to some information about registered voters; and the information that is available usually includes current address – a piece of information that is particularly important to survivors who are concerned about their privacy and safety.

Generally, almost all voter records include name, address, and party affiliation (if registered with a party). Voter records that are shared with political campaigns may also include additional personally identifying information. Some states have prohibitions on sharing certain types of information, such as social security
number or date of birth, but these limitations vary and some states don’t have any restrictions at all.

Several states allow personal information to be withheld from being shared if it is specifically designated as confidential. At least 29 of the 39 states that have Address Confidentiality Programs (ACPs)\(^1\) prevent the sharing of their participant’s voter records to keep survivors’ addresses from being sold and accessible in voter lists. Many ACPs have significant challenges effectively controlling this data, however, so it is not a guarantee of privacy. A few states also limit the sharing of residential address information for certain professions, such as police or judges.

In addition to selling voter records, every state has a process for voters to check their registration status. These status checks can be done online by filling out a form with minimal personal information, such as name and zip code. The status checks often reveal the full current address of the voter. For survivors whose address privacy is connected with their safety, these easily accessible status checks can be a scary safety risk.

What makes this issue even more difficult is the existence of “Enhanced Voter Records,” which are compiled by data brokers who collect additional individual information to make voter records even more identifying. “Enhanced Voter Records” are frequently marketed to political campaigns and may include information on voter’s purchasing habits, religious affiliation, recreational activities, and even public social media profile information.

**The New Trend: Automatic Voter Registration**

It’s important for survivors to be fully aware of how their voter information is used, shared, or sold in their state so they can make informed decisions over their privacy and safety when registering to vote. Some states are trying to increase

---

\(^1\) Address Confidentiality Programs (ACPs) are programs administered by individual states enabling victims of domestic violence, and sometimes victims of sexual assault and/or stalking, to keep their current address hidden and use an alternate mailing address for a variety of public and official processes.
voter registration by implementing, or considering the implementation of, Automatic Voter Registration (AVR), which may impact survivors who are concerned about their privacy.

AVR will make two major changes to the voter registration process. The first is that eligible citizens will be registered to vote as they access services from certain government agencies unless they decline. The second is that those agencies will transfer voter information electronically to election officials. In most states that have implemented, or are considering, AVR, the main governmental agency involved in registering voters will be the Department of Motor Vehicles (DMV). Many other states are also considering expanding the government agency registering voters to include social service agencies so that people can be registered when they apply for benefits, such as food stamps or housing programs.

AVR legislation has passed in California, Vermont, Oregon, and West Virginia. Connecticut will be implementing AVR through administrative policy – an MOU between the DMV and the Secretary of State’s Office. Many other states have considered or are considering passing legislation on AVR.

Implementation of AVR differs among states, primarily in whether it’s an opt-in or an opt-out process and where in the process that choice is made. For example, in Oregon, people who interact with the DMV will get a follow-up letter in the mail explaining AVR and they must respond within a certain timeframe in order to opt-out of being registered. Alternatively, in California, voters can decide whether to register or not while at the DMV.

Although the goal of AVR – to increase voter registration – is commendable, all voters need to be made aware of what is public information and any possible privacy protections, so that survivors can assess any privacy risks associated with being automatically registered. Once registered, their personal information may be obtainable by the public, accessible online, or available for purchase. All
eligible voters should be informed of the process to opt-out or enroll in any available address confidentiality or voter privacy program.

**The Struggle to Maintain Privacy**
For survivors and others concerned about their privacy (especially the privacy of their current home address), it’s critical that the voter registration process include up-front information so individuals are fully aware of what privacy risks exists when they register to vote. Many people do not realize that their voter registration record may be publicly available online and that it may include identifying information. Voters should also be given more options to maintain their privacy when registering to vote. These options should either be created or enhanced so they are easily accessible and available to eligible voters.

Currently, survivors who have high privacy risks have few options and may consider choosing not to register to vote to keep their address from becoming publically available. Lack of privacy is an extremely unfortunate reason for someone to not be able to vote and something that should be addressed so that all citizens can exercise their constitutional right and engage in the political process. If your state currently does not offer any type of privacy options for individuals, it’s important to explore these options.

©2017 National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVW Grant # 2014-TA-AX-K060. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit [TechSafety.org](http://TechSafety.org) for the latest version of this and other materials.