Emilie Schulz
http://www.emilieschulz.com

U.S. Voter Registries and Questions of Privacy

Voter registries are public records that states and localities make available to the public, usually for a fee, but modern technology makes using and sharing this data easier than ever before and increases the risk to voters' privacy. In October 2010, Utah candidate for U.S. Senate Mike Lee and his campaign sent emails to citizens throughout Utah. These emails included an attachment with the names, phone numbers, and addresses of Utah voters who had voted in presidential elections, but not mid-term elections. Lee and his campaign asked recipients to "challenge" their neighbors and to help them understand the importance of mid-term elections. (Pugmire, 2010). These emails violated the privacy of hundred of voters.

Voter information is accessible one of two main ways: 1) through the states and localities that maintain voter registries, and 2) through companies that purchase voter registries and then resell the information. While there are some federal laws that regulate voter registration, such as the National Voter Registration Act of 1993, the information that is required to register to vote differs from state to state. Information such as birth date, contact phone, social security number (partial or full), party affiliation, and race maybe required, optional, or not even requested depending on the state in which one is registering, and, once that information is given, it becomes part of the public record. Several jurisdictions supplement the self-provided information in each voter's record with data such as turnout history or the number of registered voters per household. (Alexander & Mills, 2004, pp. 56-59). This information is available by simply requesting it and paying any requested fees, as little as $150 for the statewide registry in Vermont or over $7,000 for Montana's statewide voter rolls. (*Id.*, pp. 57-58). In many states, it is nothing more than this financial burden that prevents anyone from requesting and obtaining voter records, although some states also regulate how the information can be used by mandating that it can only be used for political or governmental purposed, or stating that it can only be used for "non-commercial purposes." (*Id.*, pp. 56-59). Once the information has been

requested, most states choose to suppress certain data, the most common being social security number. Once again, however, there is no standard for what states choose to withhold, and some states, such as Delaware (whose form includes the optional submission of a *full* social security number), choose to suppress no data. (Alexander & Mills, 2004, pp. 52, 56). Delaware's maintenance of the voter rolls is, in fact, a troubling example of how some states regulate access to the information available in voter records: Their voter registration form requires date of birth, and optional fields for full social security number and home phone number in addition to the standard full name and address requirements, however the form includes no notice that this information will become public record and Delaware allows for any use of the data once it has been obtained. (*Id.*).

State records are not the only option for those who wish to obtain voter registration information – several companies, as well as the Democratic and Republican political parties, maintain databases of aggregate data from different states, and sometimes from other sources as well. The largest and most detailed of these databases is maintained by Aristotle, Inc., which claims Rudy Giuliani, Bill Clinton, and John McCain among its client list. (Verini, 2007). The company released, in 2007, their Aristotle 360 database which contains data on tens of millions of American voters. (*Id.*). However, this data goes far beyond what is found in the registration records maintained by states to include photos of voters, occupations, approximate income, whether one owns a gun or what type of car they drive, and more. (*Id.*). With as much information as Aristotle, Inc. has on any one voter, none of this voluntary and it is impossible for a person to access their record to review it and make changes to incorrect information – a clear violation of fair information practices. Furthermore, while Aristotle has claimed that it only sells the data to politicians and the government for election purposes, information from the Federal Election Commission shows that Aristotle, Inc. also sells its data to commercial clients, such as U.S. Bancorp. (Verini, 2007).

With so much variability in who stores voter data, how it is regulated, and who can legally access it, the opportunity for problems is great. The Mike Lee is an excellent example of how minimal regulation can be abused. Utah allows voter data to be used for a myriad of reasons, commercial and non-commercial, but, in this instance, Mike Lee is a politician campaigning to win an election. While the question of whether or not voter registries should be used for commercial or non-political purposes should be addressed, many would agree that using this information to help campaigning politicians reach their audience is appropriate. Yet, how Mike Lee had chosen to use the data calls into question whether unfettered use should be allowed even for politicians. Was it right for him to share this data with other constituents? Should voter rolls even include information about how frequently a person votes?

Even in states where voter data is limited to tightly regulated political use only, breaches like what happened in Utah can occur. In October 2009, a Virginia non-profit group, the Know Campaign, was preparing a mailing based on voter registration data. (Kunkle, 2009). This mailing was meant to encourage people to vote by implying that their voting habits could be scrutinized and judged. (*Id*.). According to Virginia state law, the Know Campaign was allowed to access the general voter data, but should not have been able to access the voting histories, as those are limited to candidates, party chairmen, and elected officials. (*Id.*). The Know Campaign says they purchased their voter rolls from a private company, highlighting another breakdown in the protection of voter data. Companies, like Aristotle, Inc., are not bound by the same laws that bind the election commissions in various states and localities, so there is nothing preventing them from selling data to individuals who are not supposed to access it.

While the examples above draw attention to clear problems in the security and privacy of voter data, both of the states involved do have laws on the books that try to protect voters and their information. Some voters are not so fortunate as to live in states where access to their data is limited

in anyway. Two prominent examples discovered in researching the issues come from North Carolina and Delaware. In both of these states, voter data can be used for any purpose commercial or political and, as a consequence is available to anyone. In North Carolina, for example, many localities, including Durham and Wake counties, make it possible to download comma delimitated text files with voter names, addresses (residential and mailing), party affiliation, gender, race, and more. (*See* Durham County Government, North Carolina, 2010; Wake County Government, North Carolina, 2010). There are no passwords or other forms of authentication that one must use to access these files.

Delaware charges for access to its voter rolls, so they are not available for download online, but can be easily ordered using an online catalogue that describes the types of reports and the cost of obtaining them. (*See* State of Delaware Government, 2010). This extra step does make the collection and use of voter data from Delaware more burdensome for someone wishing to use it for nefarious purposes, but it is still easily available for large data mining companies and similar outfits which traffic in data. Unlike North Carolina, Delaware does not consider date of birth private information and includes it as part of the data request. Furthermore, Delaware's voter registration forms include a place for people to include their social security numbers when registering[1], and their sample reports include a column for "SSN" implying that, should one include their social security number when registering, it would be made available to those who purchased the voter reports. (*See* State of Delaware Government, 2010).

Having highlighted several real concerns related to voter registries and databases, it becomes necessary to discuss how a delicate balance can be found and maintained between the need to protect

[1] Several states make it optional for voters to include their social security number when registering, but no state requires this information. Furthermore, a 1993 Appeals case, *Greidinger v Davis*, 988 F.2d 1344 (4th Cir. 1993), makes it unconstitutional to *require* a social security number to vote. It does not, however, make it unconstitutional or rule that it violates an individual's right to vote if a social security number, if provided, is made part of the public record, accessible to those who request the voter registrations lists. (*Greidinger v Davis,* 988 F.2d 1344, 1345 (4th Cir. 1993)).

personal information and the value and benefit many politicians and advocacy organizations gain from accessing voter data. While there are many things that can be done, there are three immediate solutions that should draw policymakers focus. First, companies like Aristotle, Inc and the political parties who maintain large voter databases should be regulated. Second, there should be a federally mandated minimum on what voter registration data should be considered protected. Third, voters should be educated about voter databases and issues surrounding their rights as voters when it comes to the protection of their data.

The market for aggregate data is not new, and with the Internet it has become even easier for companies to mine data and provide consumers, usually large companies, with access to databases of full of the private details of people's lives. While there are laws that do regulate these companies and the privacy rights of individuals, Aristotle, Inc and the owners of similar databases should be subject to different, and tougher, rules. At the very least, Aristotle, Inc should be required to follow the toughtest restrictions in place among the states regarding who can access voter rolls and what they can be used to accomplish. Based on a review of The California Voter Foundation's report *Voter Privacy in the Digital Age*, this would likely mean that Aristotle would be allowed to only release data only to those who are planning to use it for political and election purposes and that they would have to withhold the following information when giving people access to their data: birthdate, birth place, social security numbers (full and partial), drivers' license number, phone number, and voter ID number. (Alexander & Mills, 2004, pp. 56-59).

However, before such a policy is put in action, it would be wise of policymakers to consider whether or not to create minimum standards dictating what data can and cannot be released from voter rolls. By creating this type of standard, both consumers of voter data and well as the voters themselves would find it easier to understand and follow their rights related to voter registration data. In addition to making it illegal to share data such as social security number, birthdate, and driver

license number, this law should also establish a process for record suppression requests. At this time, some states do allow citizens to request that their voter records be withheld, although how this is done varies from anyone being able to make this request to such an option being available only to certain types of voters. For example, in Washington state, victims of domestic violence or stalkers may apply to vote using absentee ballots and have their voter records removed from any list made publicly available. (*Address Confidentiality for Victims of Domestic Violence, Sexual Assault, and Stalking,* Rev. Code of Washinton § 40.24.060 (1991)). A federal law that institutes minimum standards for withholding data from voter records should also consider instituting some minimum standards for when a voter can request to have their entire record suppressed. This law should only establish a minimum set of requirements for the protection of voters, and then allow states to withhold additional data as is considered appropriate.

While creating laws that hold those who maintain voter databases is an important step towards improving the security of voter data and protecting individual privacy, it needs to be partnered with better citizen education about voter data, their status as public records, and citizens' rights. Most people do not know that their voter records are publicly accessible or, if they do, that there are limits to how they may be used. Implementing a voter education program which could include commercials, op-eds in major news papers, and handouts that are given to individuals when they register to vote.

Voter registration records have always been considered public records, and have been used to great benefit by politicians throughout history. However, the Internet and modern communication tools have made made it easier for this data to be misused or shared with people who have no reason to access the data. With a varied map of state laws and regulations, it becomes increasingly difficult for voters to know their rights and easier for others to find the loopholes in these regulations. By instituting some policies at the federal level that establish minumum requirements for what can and

cannot be released as public records as well as extending existing laws so that they apply to companies that traffic in voter records many of the potential risks to privacy can me mitigated. Furthermore, an aggressive educational campaign would make it possible for individuals to better understand the voter records laws and help keep those who provide and use these records accountable.

Works Cited

Address Confidentiality for Victims of Domestic Violence, Sexual Assault, and Stalking, Rev. Code of Washinton § 40.24.060 (1991)).

Alexander, K., & Mills, K. (2004, June). *Voter Privacy in the Digital Age*. Retrieved October 24, 2010, from California Voter Foundation: http://www.calvoter.org/issues/votprivacy/pub/0504voterprivacy.pdf

Durham County Government, North Carolina. (2010, September 20). *VR Database*. Retrieved October 31, 2010, from Durham County Governmnet: The Official Website: http://www.co.durham.nc.us/departments/elec/VR%20Database/VR%20Database.html

Greidinger v Davis, 998 F.2d 1344 (4th Cir. 1993).

Kunkle, F. (2009, October 30). *Va. investigates legality of access to voter list*. Retrieved October 28, 2010, from Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2009/10/29/AR2009102904427.html

Pugmire, G. (2010, October 19). *E-mail from Mike Lee campaign puts voter privacy in question*. Retrieved October 24, 2010, from Daily Herald: http://www.heraldextra.com/news/local/article_f35f0617-2565-5763-b866-0e7d71e73d0d.html

State of Delaware Government. (2010, March 03). *Purchase Voter Registration Reports*. Retrieved October 31, 2010, from State of Delaware: The Official Website of the First State: http://elections.delaware.gov/services/candidate/purchasereports.shtml

Verini, J. (2007, December 13). *Big Brother Inc.* Retrieved October 24, 2010, from Vanity Fair: http://www.vanityfair.com/politics/features/2007/12/aristotle200712?printable=true&currentPage=all

Wake County Government, North Carolina. (2010, September). *Data Downloads*. Retrieved October 31, 2010, from Wake County Board of Elections: http://www.wakegov.com/elections/8data.htm