April 19, 2019

THE FUTURE OF DATA PRIVACY?

***Veronika Velch**, Associate Fellow for National Security*
***Sarah Hunt**, co-founder and CEO of the Joseph Rainey Center for Public Policy*

Personal data about individuals in several countries is being bought and sold as a commodity without the individuals' knowledge or consent. In many cases, this violates national election law. In every case, it violates the ethical norms of privacy and informed consent.

In Canada, parties used door-to-door canvassers to collect sensitive personal data without the knowledge or consent of the people whose data was collected. Three major political parties were recording "information uploaded by door-to-door canvassers detailing religious objects in voters' homes and their perceived ethnicity to create data profiles," according to a report issued by British Columbia's Office of Information and Privacy Commissioner (OIPC). None of the people whose homes were profiled had consented to it, and most were completely unaware that the canvassers had been collecting information based on their home furnishings.

Canadian law includes critical data privacy protections for citizens. The Personal Information Protection Act (PIPA) grants citizens the right to know which parties have data on them, what data those parties have collected, and which other organizations that data has been shared with.

PIPA also requires political parties to obtain informed consent from individuals before collecting data on them. Unfortunately, parties have largely failed to ask permission before collecting specific data points.

One British Columbia voter, Andrew MacLeod, requested his PIPA file and found that the Green Party knew is address, work phone number, Twitter handle, and gender – and had shared that information with 53 people and 11 other organizations. MacLeod's story is not unique; data security problems are a global issue.

Consider the 320,000 Facebook users who took a personality quiz using an app called "Thisisyourdigitallife." Cambridge Analytica is accused of harvesting that data, without the users' consent, to create voter profiles. The app also pulled data like photos, messages, and friends' profile information from users who took the personality quiz. People who took the personality quiz never had the opportunity to consent to having their data collected and shared.

Data privacy means more than being asked to "accept the terms and conditions" of an online platform. This system, called "notice and choice," was designed to give people the right to know what will happen to their data, but it fails because very few people have the time, motivation, and ability to comb through huge legal texts. Most people will check a box giving their approval without knowing what they are really agreeing to. For this reason, Center for Democracy and Technology president Nuala O'Connor told a Congressional subcommittee that "notice and choice are no longer a choice." The current system keeps consumers in the dark.

Improper data collection is only part of the problem: Data is being stored and shared improperly, too.

In the British Columbia OPIC report, "All three parties told…investigators they disclose the email addresses of known supporters to companies like Facebook." The parties did not have consent to do this.

The same problem persists in the U.K. The U.K. Information Commissioner's Office issued a report to Parliament on the state of digital data privacy. The report found that political parties routinely purchase email lists and voter data without doing due diligence on how that data was obtained. It also found that parties work with outside groups like Cambridge Analytica, without much oversight into how those outside organizations are managing voter data.

It only takes one person to put sensitive information in the hands of malicious actors. President Trump's former campaign manager Paul Manafort allegedly mishandled a massive trove of voter data by sharing polling results with Konstantin Kilimnik, a Russian associate who the FBI has identified as a Russian intelligence operative. The United States has very little legislation in place to prevent unethical data collection and sharing. In the U.S., every state has its own policy on what sort of voter data the state government will release to campaigns. There is very little oversight of how private companies collect, buy, and sell personal information.

Consent is a critical part of voter data privacy protection. Campaigns need to tell people what data they want to collect, record their answers, and respect their wishes. This starts at the top but must extend all the way to canvassing volunteers.

When those laws are in place, enforcement will be critical. Data privacy laws mean nothing unless violators face consequences. When data privacy compliance becomes part of every campaign, not just an ethical option, every voter will be able to have more trust in the integrity of the electoral system.

This article was previously published on Protego Press. For more analysis and commentary on data privacy and other technology issues, go to raineycenter.org.