CAMBRIDGE ANALYTICA AND VOTER PRIVACY

Patrick Day*

CITE AS: 4 GEO. L. TECH. REV. 583 (2020)

TABLE OF CONTENTS

I. INTRODUCTION

Finding a silver lining associated with Cambridge Analytica can be difficult. The notion of a private organization using licit and illicit means to

* Former Counsel for national security, U.S. Senate Judiciary Committee, J.D., Washington College of Law at American University; M.A., National Defense University. I am deeply thankful to Professor Julie Cohen and Alexandra Givens, from the Institute for Technology Law & Policy at Georgetown Law School; as well as Kelly McCluer, Jordan Patrick Cohen, Molly Rosen, Andrew Do, Florence Noorinejad, Gabriel Khoury, Haris Vrahliotis, Nicole Fulk, May Yang, and Joshua Banker of the *Georgetown Law Technology Review* for their helpful edits. Any mistakes herein are my own.

undermine elections around the world for profit is hard to reconcile with liberal democratic values. A *brief* sampling of the myriad allegations against the U.K.-based data analytics firm include: sharing detailed information on U.S. voters with Russian intelligence;[1] working with a far-right U.K. politician suspected of Russian ties on the Brexit campaign;[2] participating in a scheme to hack a Nigerian presidential candidate's personal emails on behalf of "oil billionaires";[3] meeting with Julian Assange of Wikileaks while he possessed Hilary Clinton's emails stolen by Russian intelligence;[4] and secretly recording a candidate receiving a fake bribe offer in an election in St. Kitts and Nevis.[5] Most of these activities occurred during the same period that Cambridge reportedly worked in more than forty-five elections in the United States,[6]

---

[1] Carole Cadwalladr & Emma Graham-Harrison, *Cambridge Analytica: Links to Moscow Oil Firm and St Petersburg University*, GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university [https://perma.cc/Q4Q2-LXZA]; *see also Cambridge Analytica and the Future of Data Privacy*: *Hearing before S. Comm. on the Judiciary*, 115th Cong. (2018) (statement of Sen. Diane Feinstein, Ranking Member, S. Comm. on the Judiciary).

[2] Luke Harding, *Investigators Bound to Scrutinise Arron Bank's Russian Links* (Nov. 1, 2018), https://www.theguardian.com/uk-news/2018/nov/01/investigators-will-scrutinise-arron-banks-russian-links [https://perma.cc/WP7B-2HWX]; Mark Scott, *Cambridge Analytica Did Work for Brexit Groups, Says Ex-Staffer,* POLITICO (July 7, 2019), https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/ [https://perma.cc/U6ZX-WLEU];; *The Banks Files: How Brexit 'Bad Boy' Arron Banks Was Eyeing a Massive Russian Gold Deal*, CHANNEL 4 NEWS (Mar. 5, 2019), https://www.channel4.com/news/the-banks-files-how-brexit-bad-boy-arron-banks-was-eyeing-a-massive-russian-gold-deal [https://perma.cc/KQ6D-9D2D].

[3] Yomi Kazeem, *Cambridge Analytica Tried to Sway Nigeria's Last Elections with Buhari's Hacked Emails*, QUARTZ AFRICA (Mar. 22, 2018), https://qz.com/africa/1234916/cambridge-analytica-tried-to-sway-nigerias-last-elections-with-buharis-hacked-emails/ [https://perma.cc/6J5B-J6CA]; Paul Lewis & Paul Hilder, *Former Cambridge Analytica Exec Says She Wants Lies to Stop*, GUARDIAN (Mar. 23, 2018), https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies [https://perma.cc/4XBV-PQFV].

[4] Carole Cadwalladr & Stephanie Kirchgaessner, *Cambridge Analytica Director 'Met Assange to Discuss US Election,'* GUARDIAN (June 7, 2018), https://www.theguardian.com/uk-news/2018/jun/06/cambridge-analytica-brittany-kaiser-julian-assange-wikileaks [https://perma.cc/4APT-P5CT]; *see also* Michael S. Schmidt, *Trump Invited the Russians to Hack Clinton. Were They Listening?*, N.Y. TIMES (July 13, 2018), https://www.nytimes.com/2018/07/13/us/politics/trump-russia-clinton-emails.html [https://perma.cc/L49B-F8NJ].

[5] April Glaser, *How Shady was Cambridge Analytica?*, SLATE (Mar. 29, 2018), https://slate.com/technology/2018/03/cambridge-analyticas-work-in-the-caribbean-was-pretty-shady.html [https://perma.cc/A87L-FFF9].

[6] Frances S. Sellers, *Cruz Campaign Paid $750,000 to 'Psychographic Profiling' Company*, WASH. POST (Oct. 19, 2015), https://www.washingtonpost.com/politics/cruz-campaign-paid-

including on behalf of three major-party candidates for president.[7] Many of Cambridge Analytica's former clients now occupy elected or appointed positions in the U.S. government,[8] and several former employees work in American politics, including for the current President's reelection campaign.[9]

However, without the famous undercover video of Cambridge's CEO offering to use Ukrainian prostitutes and bribes to undermine another foreign election,[10] the public would not have had access to the wealth of information now available about Cambridge Analytica, particularly its attempt at "psychological persuasion"[11] of U.S. voters.[12] Publicly, Cambridge Analytica described its voter targeting process as follows: "[building] on top of demographic polling and traditional microtargeting with an extra dataset on personality, and we use that in order to understand the behavioral drivers that allow us to change voting behavior."[13] Privately, it used psychographic profiles on 230 million Americans to conduct what the firm called "'psychological operations,' or psyops – [which change] people's minds not through persuasion but through 'informational dominance', a set of techniques

750000-to-psychographic-profiling-company/2015/10/19/6c83e508-743f-11e5-9cbb-790369643cf9_story.html [https://perma.cc/G9P5-BSHG].

[7] The following Republican Party Presidential Candidates were clients of Cambridge Analytica: Ted Cruz, Ben Carson, and Donald Trump. Maegan Vazquez & Paul Murphy, *Trump Isn't the Only Republican Who Gave Cambridge Analytica Big Bucks*, CNN (Mar. 21, 2018), https://www.cnn.com/2018/03/20/politics/cambridge-analytica-republican-ties/index.html [https://perma.cc/3W45-HJH2].

[8] The following U.S. government officials were reportedly clients of Cambridge Analytica: Ben Carson, Steve Bannon, John Bolton, Thom Tillis, and Tom Cotton. *Id.*

[9] The following former Cambridge Analytical employees now work on the current President's re-election campaign or for the Republican National Committee: Matt Oczkowski and Alex Lundy. Alex Isenstadt, *Trump Campaign Hires Alum of Controversial Data Company*, POLITICO (Feb. 19, 2020), https://www.politico.com/news/2020/02/19/trump-cambridge-analytica-oczkowski-114075 [https://perma.cc/NV2H-CG85] (Matt Oczkowski works for Data Propria, which has been retained by Donald Trump's 2020 reelection campaign); Alex Isenstadt, *RNC Rehires Firm Responsible for Massive Data Breach*, POLITICO (Mar. 20, 2020), https://www.politico.com/news/2020/03/20/rnc-deep-root-analytics-hire-138889 [https://perma.cc/UYJ7-C4YH] (Alex Lundry was recently hired by the Republican National Committee).

[10] *Data, Democracy and Dirty Tricks*, CHANNEL 4 NEWS (Mar. 19, 2018), https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose [https://perma.cc/W6AZTTY2].

[11] Wu Youyou et al., *Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans*, 112 PROC. NAT'L ACAD. SCI. 1036 (2015).

[12] Kenneth Vogel & Tarini Parti, *Cruz Partners with Donor's 'Psychographic' Firm*, POLITICO (July 7, 2015), https://www.politico.com/story/2015/07/ted-cruz-donor-for-data-119813 [https://perma.cc/7YHK-F4WS].

[13] Cambridge Analytica, *Cambridge Analytica @ Reboot Conference*, YOUTUBE (Aug. 15, 2015), https://www.youtube.com/watch?v=p_H0DLvMD-0 [https://perma.cc/N465-G82U].

that includes rumor, disinformation and fake news."[14] Prior to the undercover footage, and whistleblowers like Christopher Wiley, Cambridge Analytica was celebrated as an "up and coming company with technology not to be missed."[15]

Fortunately, Cambridge Analytica has now been subject to government investigations on five continents,[16] documentaries,[17] and two years of award-winning investigative journalism.[18] Public outrage regarding the firm's activities led many Americans to question for the first time the economic and national security costs associated with U.S. social media platforms' data harvesting.[19] And, after years of resisting lawmakers' requests, Facebook CEO Mark Zuckerberg was compelled to testify before Congress for the first time.[20]

The Cambridge Analytica affair also resulted in the introduction of the first federal legislation in the United States that would regulate the use of voters' personal information in elections—the Voter Privacy Act of 2019. According to the bill's sponsor, U.S. Senator Dianne Feinstein (D-CA), the Voter Privacy Act of 2019[21] is a direct response to Cambridge Analytica and is intended to mitigate "sophisticated online surveillance" by candidates and campaigns intended to target and influence voters' "unique psychological characteristics."[22]

---

[14] Carol Cadwalldr, *I Made Steve Bannon's Psychological Warfare Tool: Meet the Data War Whistleblower*, GUARDIAN (Mar. 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump [https://perma.cc/5H56-ZK3R].

[15] *Id*.

[16] *Cambridge Analytica and the Future of Data Privacy*: *Hearing before S. Comm. on the Judiciary*, 115th Cong. (2018) (prepared statement of Sen. Diane Feinstein, Ranking Member, S. Comm. on the Judiciary) ("numerous governments have launched formal investigations into the company including the United Kingdom, Australia, Canada, Nigeria, Kenya, and India").

[17] *See, e.g.*, THE GREAT HACK (Netflix 2019).

[18] *See The Cambridge Analytica Files*, GUARDIAN https://www.theguardian.com/news/series/cambridge-analytica-files [https://perma.cc/XM96-GR6X].

[19] *See, e.g.*, Kari Paul, *A Brutal Year: How the 'Techlash' Caught Up With Facebook, Google, and Amazon*, GUARDIAN (Dec. 28, 2019), https://www.theguardian.com/technology/2019/dec/28/tech-industry-year-in-review-facebook-google-amazon [https://perma.cc/CKV8-ZY62].

[20] *Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before S. Comm. on the Judiciary and S. Comm. on Commerce, Science and Transportation*, 115th Cong. (2018) (statement of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook).

[21] Voter Privacy Act of 2019, S. 2398, 116th Cong. (2019).

[22] Press Release, U.S. Senator Diane Feinstein, Feinstein Bill Would Give Voters Control Over Personal Data (July 31, 2019), https://www.feinstein.senate.gov/public/index.cfm/press-

Clearly, Cambridge Analytica captured the attention of regulators and the public, particularly regarding the use of data in elections. But as Ira Rubenstein described in *Voter Privacy in the Age of Big Data* in 2014, the application of Big Data, behavioral advertising, and advanced data analytics techniques are not necessarily new in political campaigns. Political parties have been some of the earliest adopters of sophisticated online data analytics dating back to the 2004 Presidential election.[23] Rubenstein observes that major political parties may be the "largest assemblages of personal data in contemporary American life."[24]

As a result, whether the Voter Privacy Act is signed into law or not, at some point courts will likely consider the constitutionality of regulating the use of personal information in elections. Moreover, given the volume of information now in the public record regarding Cambridge Analytica's use of computational means to discern, analyze, and manipulate voter's underlying psychological characteristics, there is an additional question as to whether those techniques could reach a level of scientific efficacy for the court to find them violative of fundamental rights like individual liberty and popular sovereignty.

To that end, the following will review Senator Feinstein's proposed Voter Privacy Act and potential legal obstacles associated with regulating the use of voters' personal information in elections, as well as the techniques used by Cambridge Analytica and whether they could change courts' views of voter privacy in the Digital Age.

II. THE VOTER PRIVACY ACT

The proposed Voter Privacy Act of 2019[25] is not only the first federal legislation that would regulate the use of voters' personal information in elections, but its provisions seem intended to shape future litigation regarding voter privacy. Broadly, the bill would amend the Federal Election Campaign Act of 1971 (FECA) to provide voters with legal rights to control the use of their personal information by political entities, which are defined as candidates, political committees, national committees, and political parties under the FECA as well as political organizations under Section 527 of the Internal Revenue Code.[26] The bill also applies to any person using voter

releases?id=B4FBA307-B050-4623-8EAF-841DCDCAFDA4 [https://perma.cc/2GJQ-HFAJ].

[23] Ira Rubenstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 5, 861, 876 n.76 (2014).

[24] *Id*. at 861.

[25] Voter Privacy Act, *supra* note 21.

[26] *Id.*

personal information to carry out regulated campaign activities under the FECA, including public communications, mass mailing, or telephone banking.[27] Voters' data ownership rights would be enforced by the Federal Election Commission, including via civil and criminal sanctions.[28]

A. Findings and Sense of Congress

The bill's *Congressional Findings* attempt to shape future litigation in two ways: (1) by providing sufficient factual detail to allow a court to find that modern voter targeting techniques are materially different from historic political advertising; and (2) in its role as the representatives of the public, clearly articulating Congress's assessment of the public's interest in regulating such activity rather than leaving it to the court.

To support subsequent provisions, the bill provides significant detail and resources on the following factual themes: dramatic growth in Internet usage in the United States; proliferation and depth of data collection by online platforms; advancement of new surveillance techniques such as real-time recording of an individual's browsing sessions; the ability to infer private information that was never revealed publicly; the incorporation of neurological research into online advertising techniques designed to manipulate users' "precognitive functions"; the adoption of behavioral advertising and microtargeting techniques by U.S. political entities; and Cambridge Analytica's use of voter's personality traits to conduct psychological operations to alter voter behavior.[29]

The sense of Congress also explicitly states the government's interest based on the foregoing facts: "It is the sense of Congress that . . . the Federal Government has a compelling interest in protecting voters from surveillance and manipulation;" that the bill is "the most narrowly tailored approach to protecting voters from psychological manipulation;" and that the "Federal Government's interest would justify additional prohibitions" if necessary.[30]

Congressional findings are not only relevant for courts in determining legislative judgement,[31] but also in "advanc[ing] judicial review by identifying the factual authority on which Congress relied."[32] In addition, there is at least some indication that the amount of data provided by Congress could be dispositive in a difficult balancing of competing interests.[33]

---

[27] *See* 52 U.S.C. § 30101(21).
[28] Voter Privacy Act, *supra* note 21, at § 358*; see also id.* at 354(e)(2).
[29] *Id.* at § 2.
[30] *Id.* at § 3.
[31] United States v. Morrison, 529 U.S. 598 (2000).
[32] *Id.* at 628 (Souter, J., dissenting).
[33] *Id.*

B. Rights Provided Under the Act

Similar to the European Union's General Data Protection Regulation (GDPR)[34] and the California Consumer Privacy Act (CCPA),[35] the Voter Privacy Act would allow voters to control the use of their personal information via certain codified rights: (1) right of access, (2) right of erasure, (3) right to prohibit transfer, (4) right to notice, and (5) right to prohibit targeting.[36] Collectively, these rights allow voters to dictate how their information is used by covered entities, though voters are required to act affirmatively. The only right in the bill that is self-executing is the right of notice, which requires covered entities to notify voters as soon as they take possession of voters' personal information.

One of the Voter Privacy Act's novel components is its prohibition on targeting by third-party websites on behalf of covered entities. The provision is similar to Twitter's recent announcement that it no longer accepts political advertisements on its platform.[37] As has been the source of some confusion, Twitter's ban on political advertising does not preclude politicians from using the platform, including for political messaging.[38] Rather, Twitter will no longer allow political entities to purchase its ad-targeting services that use sophisticated user data profiles to force ads into individuals' Twitter feeds.[39]

The Voter Privacy Act's prohibition on targeting seems to work similarly to Twitter's policy. It would allow individuals to opt out of permitting third-party websites to use their personal information for ads targeted on behalf of a covered entity. For example, an individual could log onto Facebook, go to their privacy settings, and opt out of receiving targeted ads from covered entities. The provision would not limit covered entities' ability to send out ads on third-party websites, nor would it limit the total number of online ads a covered entity could send. It would only limit covered entities' ability to use personal information to target its online ads. Notably, the bill does not include information derived from state voter registration databases in its definition of personal information. As a result, covered entities

---

[34] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119/1) (hereinafter "(General Data Protection Regulation").
[35] CAL. CIV. CODE § 1798 et seq. (2018).
[36] Voter Privacy Act, *supra* note 21, at § 4.
[37] Anthony Ha, *Jack Dorsey Says Twitter Will Ban All Political Ads*, TECH CRUNCH (Oct. 30, 2019), https://techcrunch.com/2019/10/30/twitter-political-ad-ban/ [https://perma.cc/3TEZ-VRQZ].
[38] *Id.*
[39] *Id.*

could still target online ads, even if a voter opts out, based on data like party affiliation, address, and zip code.[40]

One clear difference between the Voter Privacy Act and other data protection statutes like the GDPR is that the bill does not generally include front-end "use restrictions."[41] The GDPR limits covered entities to six exclusive, authorized uses for individual personal information. The authorized uses describe general categories of activity like consent that is necessary for the performance of a contract or necessary for performance of a legal duty.[42] Any collection, use, or processing of personal information inconsistent with an approved use is prohibited. The Voter Privacy Act has no such restriction. Political entities are not subject to any blanket prohibition on collection, use, or processing of any voter's data. The only limitation a covered entity would encounter would be from the voter themselves, and only with respect to that voter's own personal data.

The lone use restriction on data transfer in the legislation is a prohibition on transferring voters' personal information outside of the United States.[43] There is no specific explanation for the provision. However, given that Senator Feinstein indicated on numerous occasions that the bill was intended to respond to Cambridge Analytica, one possible reason for the provision could be a response to reports that Cambridge Analytica passed U.S. voter information to the state-owned Russian oil firm Lukoil.[44] At the Senate Judiciary Committee's hearing on Cambridge Analytica, Senator Feinstein referred to Lukoil as having a "formal information-sharing partnership with the Russian Federal Secret Service, the FSB, the successor to the KGB."[45]

C. Definitions Included in the Act

The Voter Privacy Act's definitions provide notable limitations on the overall scope of the legislation. For example, the bill defines "personal information"[46] to include ten categories of data like personal identifiers, consumer history, Internet browsing history, geolocation, personality traits, and other psychographic modeling.[47] However, it excludes publicly available

[40] Voter Privacy Act, *supra* note 21, at § 351(4)(B).
[41] General Data Protection Regulation, *supra* note 34, at Art. 6.
[42] Specifically, these authorized uses include: (1) use with consent, (2) use in performance of a contract, (3) use in compliance with another legal obligation, (4) use to protect the vital interests of the data subject, (5) use for the public interests, and (6) use for the legitimate interests of the controller. *Id.*
[43] Voter Privacy Act, *supra* note 21, at § 4.
[44] Cadwalladr & Graham-Harrison, *supra* note 1.
[45] Feinstein, *supra* note 16.
[46] Voter Privacy Act, *supra* note 21, at § 4(a).
[47] *Id.*

information, deidentified information, and aggregate polling information.[48] Publicly available information is defined as "information obtained from a Federal, state, or local voter registration database."[49]

The exclusion of information obtained from state voter registration databases is significant for two reasons. One, according to the National Conference of State Legislatures, state voter registration databases can include significant information including party registration, name, address, date of birth, occupation, and voting history.[50] Two, it ensures that candidates have access to some minimum voter data to protect their ability to effectively communicate with voters. As Rubenstein observes, some political professionals consider state voter registration data the most valuable data available in operating campaigns.[51]

III. LEGAL CHALLENGES

Endeavoring to regulate the use of personal data in elections, the Voter Privacy Act could face a number of constitutional challenges. The most likely are: (A) whether the law impermissibly limits the quantity of protected speech;[52] and (B) whether the law impermissibly restrains the individual right of candidates to access a voter's personal information.[53]

A. Limits on Quantity of Speech

The first test for any legislation that regulates political campaign activity, particularly under the Federal Election Campaign Act (FECA), is under *Buckley v. Valeo*. Following the Watergate scandal and subsequent passage of the Federal Election Campaign Act of 1974 (FECA),[54] plaintiffs in *Buckley* challenged a variety of the new campaign finance laws, including expenditure limits, contribution limits, public disclosure of contributions, and public financing of elections.[55] Expenditure limits in the Act capped the overall amount a candidate could spend during a campaign and how much an

[48] *Id.*
[49] *Id.*
[50] Rubenstein, *supra* note 23, at 868.
[51] *Id*.
[52] *See* Buckley v. Valeo, 424 U.S. 1 (1976).
[53] *See* Sorrell v. IMS Health, 564 U.S. 552 (2011).
[54] Lee E. Goodman, *The First Amendment Right to Political Privacy, Chapter 6, Campaign Finance and Other Very Public Exceptions to Privacy*, WILEY REIN LLP (Sept. 2019), https://www.wiley.law/newsletter-The-First-Amendment-Right-to-Political-Privacy-Chapter-6-Campaign-Finance-and-Other-Very-Public-Exceptions-to-Privacy [https://perma.cc/5STJ-QFSD].
[55] *Buckley*, 424 U.S. at 19–20.

individual could spend "relative to a clearly identified candidate."[56] The Court invalidated limits on expenditures finding that "a restriction on the amount of money a person or group can spend on political communication during a campaign necessarily reduces the quantity of expression by restricting the number of issues discussed, the depth of the exploration, and the size of the audience reached."[57]

The Court upheld other provisions of the FECA such as mandating disclosure of political contributions. The FECA required political committees to keep detailed records of all contributions and expenditures, including the name and address of every individual contributor over a certain dollar amount, and to publish them for public inspection. The Court found that while the provision imposed no ceiling on campaign related activities, it compelled disclosure of political activity and infringed on the "privacy of association and belief guaranteed by the First Amendment."[58] However, potentially in part because it had already invalidated expenditure limits, the Court conceded that disclosure was the least restrictive means for Congress to address the rampant corruption it had identified in political campaigns and upheld the provision.

Over the next forty years the Court would take an increasingly aggressive posture toward campaign finance regulations, invalidating provisions like limits on independent expenditures by corporations.[59] Yet, it has remained equally steadfast in upholding public disclosure requirements.[60] Outside of right-of-association cases, the only instances where the Court has retreated from its preference for disclosure over privacy were in instances where plaintiffs could demonstrate that compelled disclosure had actually resulted in physical harm.[61]

Buckley and its progeny continue to stand for the proposition that any regulation under the FECA may not restrict the *quantity* of speech. On its face the Voter Privacy Act does not appear to run afoul of that requirements. However, the Court's repeated preference for transparency at the expense of privacy is instructive on the relative weight of two interests in the context of political campaigns.

B. Limits on Candidates' Access to Data

The Voter Privacy Act could limit a candidate's access to certain voter data, which the Court has found is protected speech under the First

[56] *Id.* at 13.
[57] *Id.* at 19.
[58] *Id*. at 64.
[59] *See* Citizens United v. FEC, 558 U.S. 310 (2010).
[60] *See* McConnell v. FEC, 540 U.S. 93 (2003).
[61] Britt v. Superior Court, 20 Cal. 3d 844, 849 (1978).

Amendment. In *Sorrell v. IMS Health Inc.*,[62] the Court invalidated a Vermont statute that prohibited the sale of prescriber-identifiable information for marketing prescription drugs without the prescriber's consent.[63] The Court found that, by prohibiting access to data for a singular purpose like marketing, the statute imposed content-based, viewpoint-based, and speaker-based restrictions under the First Amendment.[64]

Finding that the regulation imposed significant restrictions on protected speech, the Court considered whether the government had articulated a substantial interest sufficient to sustain the burden. Vermont argued that the statute was necessary to protect medical privacy and to achieve several policy objectives, like improving public health and reducing health care costs.[65] The Court rejected both arguments, finding while it restricted access to marketers, that the Vermont statute permitted access to journalists, researchers, and insurers.[66] The Court also found that while the state's goals to reduce health care costs "may be proper, [the statute] does not advance them in a permissible way," namely, by "restraining certain speech by certain speakers."[67]

Sorrell continues to stand for the proposition that access to data, which can be used to improve the persuasiveness of a speaker's message, is protected under the First Amendment. Notably, Justice Kennedy did not foreclose the possibility of any regulation of personal data under the First Amendment. In his opinion, he cites data protection statutes like Health Insurance Portability and Accountability Act (HIPAA) as positive examples that did not raise the same concerns as the statute at issue.[68] However, Sorrell does continue to stand for the proposition that if a statute endeavors to regulate the use of data, it must serve a sufficiently compelling interest.

IV. IS VOTER PRIVACY A COMPELLING INTEREST IN THE DIGITAL AGE?

Whether voter privacy could be considered a sufficiently compelling interest to sustain legislation like the Voter Privacy Act is a two-part question. The first part is a factual question about whether there is sufficient data or other evidence to find a concept like voter privacy compelling on its face. The

[62] 564 U.S. 552 (2011).
[63] *Id.* at 557.
[64] *Id*. at 564–65.
[65] *Id.* at 572 ("First, the State contends that its law is necessary to protect medical privacy, including physician confidentiality, avoidance of harassment, and the integrity of the doctor patient relationship. Second the State argues that §4631(d) is integral to the achievement of policy objectives- namely, improved public health and reduced health care costs").
[66] *Id.* at 572–73.
[67] *Id.* at 577.
[68] *Id.* at 573.

second could be described as more of a question of law, but essentially it is how a court would choose to balance voter privacy against other competing rights and interests.

A. Factual Basis for Voter Privacy

Fortunately, investigations of Cambridge Analytica have provided a wealth of information regarding modern data practices by political campaigns, advances in psychographics, and the national security implications of foreign nations adopting these techniques to engineer outcomes in American elections.

1. *Modern Data Collection and Campaigns*

The Internet is an indispensable part of modern economic and social life in the United States. According to the Pew Research Center, ninety percent of Americans use the Internet.[69] From 2005 to 2019, the number of Americans using social media increased from five percent to seventy-two percent.[70] For those under the age of thirty, that figure was ninety percent.[71] Facebook has 2.4 billion daily active users globally.[72] About seventy percent of American adults have a Facebook account, and forty-three percent get their news from Facebook.[73]

As a result, the repository of personal information that is collected and made widely available by companies like Google and Facebook about each individual American citizen is materially different than any period in American history. As noted in the Voter Privacy Act:

> One U.S. based search engine advertises its ability to track hundreds of categories of data about specific individuals including age, gender, occupation, income level, sexual orientation, national origin, religion, medical conditions such as AIDs, erectile dysfunction, bipolar disorder, eating disorders, and sexually transmitted diseases, family

[69] *Internet/Broadband Fact Sheet*, PEW RES. CTR. (Jun. 12, 2019), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/ [https://perma.cc/C9DC-FG4C].
[70] *Id.*
[71] *Id.*
[72] *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2019*, STATISTA (2020), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [perma.cc/JC76-LHVR].
[73] *10 Facts About Americans and Facebook*, PEW RES. CTR. (MAY 16, 2019), https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook/ [perma.cc/GX67-AXHJ].

> information such as number of children, children with special needs, infertility, and substance misuse, and support for social issues such as reproductive rights, unions and labor issues, and support for gun rights.[74]

Every time an individual visits a website, information like the kind listed above is broadcast to tens or hundreds of companies for the opportunity to show that individual advertisements.[75] Moreover, these advertising protocols include unique ID codes "so that all of this information can be tied to you over time. This allows companies you have never heard of to maintain intimate profiles on you, and on everyone you have ever known."[76] One reporter determined that Google maintained 5.5 gigabytes of her personal data, which is roughly equivalent to 3 million word documents worth of text.[77]

Campaigns have been some of the earliest adopters of online data collection, analytics, and microtargeting. As early as 2004, major party databases included data on "every one of the 168 million or so registered voters in the country, cross-indexed with phone numbers, addresses, voting history, income range and so-on up to several hundred points of data on each voter."[78] In 2014, Rubenstein observed:

> Political databases hold records on almost 200 million eligible American voters. Each record contains hundreds if not thousands of fields derived from voter rolls, donor and response data, campaign web data, and consumer and other data obtained from data brokers, all of which is combined into giant assemblages made possible by fast computers, speedy network connections, cheap data storage, and ample financial and technical resources.[79]

Unique personalized identifiers like IP addresses, cookies, and mobile device IDs allow campaigns to integrate diverse datasets "while data mining and sophisticated statistical techniques allow them to engage in highly strategic and cost-effective analysis and targeting."[80] Because political professionals consider data dispositive in determining the outcome of

---

[74] Voter Privacy Act, *supra* note 21, at § 2(3).
[75] *Id.*, at § 5.
[76] *Id*.
[77] Dylan Curran, *Are You Ready? Here is All the Data Facebook and Google Have on You*, GUARDIAN (Mar. 30, 2018), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy [https://perma.cc/PT5X-N58D].
[78] Rubenstein, *supra* note 23, at 876.
[79] *Id.* at 879.
[80] *Id.* at 884.

elections, campaigns will continue to expand the scope of their collection, analysis, and targeting.

2. *New Developments in Psychographics*

Cambridge Analytica used large datasets and computational means to target and influence voters' underlying psychological traits to alter their behavior. The firm reportedly based its work on a series of studies published by the National Academy of Sciences that describe material advances in the field of psychographics made possible by U.S. social media platforms.[81]

Psychographics is the study and classification of people according to their attitudes, aspirations, and other psychological criteria. Whereas *demographics* measure age, education, income, gender, and race, *psychographics* measure psychological traits like personality, interests, attitudes, and beliefs. Rather than describing who a person is, psychographics attempt to illustrate why a person behaves a certain way. Psychographics were developed after World War II as researchers sought to apply concepts of clinical psychology in order to better understand consumer behavior.[82] As one scholar described, psychographic information puts flesh on the demographic bone.[83]

One of the most common psychographic measures is personality. Like most psychographics, it is a latent trait—meaning it cannot be observed directly. Instead, individual characteristics are measured through surveys and questionnaires. One of the most common methods for testing personality is the Five-Factor Model, also called the "OCEAN test." The OCEAN test categorizes an individual's personality according to the following traits: openness, conscientiousness, extraversion, agreeableness, and neuroticism.

It is well-established that persuasive appeals are more effective in influencing human behavior when they are tailored to an individual's unique personality traits.[84] However, large-scale personality-based persuasion campaigns face two limitations: cost and reliability. It would not be practical or cost effective to attempt to convince five to ten million people to sit for a one-hundred question personality test. Alternatively, focus groups can yield useful insight, but the reliability of the results can degrade with extrapolation to larger groups of diverse individuals.[85]

---

[81] Cadwalladr, *supra* note 14.
[82] William D. Wells, *Psychographics: A Critical Review*, 12 J. MARKETING RES., 196 (1975).
[83] *Id*. at 198.
[84] S.C. Matz et al., *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, 48 PROC. NAT'L ACAD. SCI. 12714 (2017), https://www.pnas.org/content/pnas/114/48/12714.full.pdf [https://perma.cc/K8KR-NQ38].
[85] *See* Wells, *supra* note 82.

Cambridge Analytica reportedly based its methodology on two recent studies published in *Proceedings of the National Academy of Sciences*, the official journal of the National Academy of Sciences. The studies suggest that personality traits can be cheaply and accurately inferred from an individual's public social media data, which can be used to conduct large-scale psychologically persuasive campaigns based on actual knowledge of each target's personality rather than estimations.

The first study found that individual's personality traits can be measured through social media data, instead of requiring a personality questionnaire. Entitled *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*,[86] the study examined 58,000 volunteers, each of whom provided Facebook Likes, demographic profiles, and the results of several personality questionnaires.[87] The resulting data was analyzed to connect Facebook Likes for topics such as "the Colbert Report," "Harley Davidson," or "Wu Tang Clan" with personality traits like "openness," as well as other attributes like sexual orientation, political views, or substance abuse.[88] Researchers concluded "basic digital records of human behavior can be used to automatically and accurately estimate a wide-range of personal attributes that people would typically assume to be private… [P]redictability of individual attributes from digital records of behavior may have considerable negative implications, because it can easily be applied to large numbers of people without obtaining their individual consent and without them noticing."[89] Subsequent studies have found success at inferring sensitive personal information from personal websites,[90] blogs,[91] Twitter messages,[92] Facebook profiles,[93] and Instagram pictures.[94] Facebook itself reportedly

[86] Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. 5802 (2013), https://www.pnas.org/content/110/15/5802 [https://perma.cc/DFD7-FF7M].
[87] *Id.*
[88] *Id.* at 5894.
[89] *Id.* at 5805.
[90] Bernd Marcus, Fraz Machilek, & Astrid Schütz, *Personality in Cyberspace: Personal Web Sites, as Media for Personality Expressions and Impressions*, 90 J. PERSONALITY & SOC. PSYCHOL. 1014, 1014–1031 (2006).
[91] Tal Yarkoni, *Personality in 100,000 Words: A Large-Scale Analysis of Personality and Word Use Among Bloggers*, 44 J. RES. PERSONALITY 363, 363–373 (2010).
[92] Jennifer Golbeck et al., *Predicting Personality from Twitter*, IEEE INT'L CONFERENCE ON PRIVACY, SEC., RISK, & TRUST 149 (2011).
[93] Gregory Park et al., *Automatic Personality Assessments Through Social Media Language*, 108 J. PERSONALITY & SOC. PSYCHOL. 934, 934–952 (2014).
[94] Crisitina Segalin et al., *The Pictures We Like are Our Image: Continuous Mapping of Favorite Pictures into Self-Assessed and Attributed Personality Traits*, 8 IEEE TRANSACTIONS ON AFFECTIVE COMPUTING 268, 268–285 (2017).

obtained a patent that described how personality characteristics like emotional stability could be determined from individuals' messages and status updates.[95]

The second study found that computers could infer an individual's personality traits more accurately than any human. Entitled *Computer-Based Personality Judgements Are More Accurate Than Those Made by Humans*, the study compared computer projections of an individual's personality with those made by the same individual's coworkers, friends, family members and spouse.[96] The study concluded that computers were "significantly more accurate than humans" at predicting an individual's personality.[97] Moreover, with only ten, seventy, one hundred and fifty, and three hundred Facebook Likes, computers could outperform an average coworker, friend, family member, and spouse respectively.[98] Researchers noted that that "growth in both the sophistication of the computer models and the amount of digital footprint might lead to computer models outperforming humans even more decisively."[99] Again, researchers warned that:

> [A]utomated, accurate, and cheap personality assessment tools could affect society in many ways … knowledge of people's personalities can also be used to manipulate and influence them. Understandably, people might distrust or reject digital technologies after realizing that their government, internet provider, web browser, online social network, or search engine can infer their personal characteristics more accurately than their closest family members.[100]

Together, the studies addressed two of the fundamental challenges of applying large-scale psychographic persuasion campaigns. First, researchers can infer the personality traits of large populations of individuals for minimal cost and without those individuals' knowledge. Second, because computer algorithms can determine the personality for each individual in a large population—rather than by generalizing from focus groups and modeling—the results can be highly accurate.

In 2017, a third study found that using inferred personality data from social media allowed researchers to alter the behavior of large groups of

---

[95] Rory Cellan-Jones, *Facebook Explored Unpicking Personalities to Target Ads*, BBC, (Apr. 24 2018) https://www.bbc.com/news/technology-43869911 [https://perma.cc/24N4-VV45].
[96] Youyou et al., *supra* note 11, at 1037.
[97] *Id.*
[98] *Id. See also* Douglas Quenqua, *Facebook Knows You Better Than Anyone Else*, N.Y. TIMES (Jan 19, 2015), https://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html [https://perma.cc/J439-B6VM].
[99] Youyou et al., *supra* note 11, at 1039.
[100] *Id.*

people in a real-world environment. Entitled *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*,[101] the study conducted three real-world experiments including 3.7 million people, targeting each individual based on their unique openness and extraversion qualities as derived from Facebook Likes. Even with a small digital footprint for each individual, matching psychologically persuasive ads to each individual's personality traits resulted in *40% more clicks* and *50% more purchases*. Researchers concluded:

> The results of these three studies provide converging evidence for the effectiveness of psychological targeting in the context of real-life digital mass persuasion; tailoring persuasive appeals to the psychological profiles of large groups of people allowed us to influence their actual behaviors and choices. Given that we approximated people's psychological profiles using a single [Facebook] Like per person—instead of predicting individuals profiles using people's full history of digital footprints—our findings represent a conservative estimate of the potential effectiveness of psychological mass persuasion.[102]

Further, researchers commented that these types of psychologically persuasive advertisements could be applied by governments, companies, or political parties "to covertly exploit weaknesses in [peoples'] character and persuade them to take action against their own best interest, [highlighting] the potential need for policy interventions."[103]

There is sufficient evidence to presume that techniques like *digital mass persuasion* can be effective in highly networked societies with large repositories of personal data. The key to both the accuracy and effect of these methodologies is the amount of data available on each subject. It is well-established that personal data is a strategic economic asset.[104] Given that personal data could also be used to engineer the outcome of an election, democracies might begin to consider it a national security asset as well.

---

[101] Matz et al., *supra* note 84.
[102] *Id*. at 12717.
[103] *Id*. at 12714.
[104] *See, e.g.*, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee for the Regions: A European Strategy for Data,* COM (2020) 66 final (Feb. 2, 2020), https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf [https://perma.cc/W2G5-SECE].

3. *National Security*

Given the Russian government's recent use of information operations to undermine American elections and their effort to obtain U.S. voter data from Cambridge Analytica directly, the U.S. government has a clear national security interest in limiting foreign access to U.S. voters' personal information.

It is well established that the Russian government conducted large-scale information operations targeting U.S. voters to help elect Donald Trump as U.S. President. On January 6, 2017, the Director of National Intelligence (DNI) released a consensus Intelligence Community assessment regarding Russian interference in the 2016 U.S. Presidential election.[105] The report concluded that Russia used a combination of government agencies, state-funded media, third-party intermediaries, and paid social media users or trolls to undermine Americans' confidence in democracy and help elect Donald Trump. The DNI concluded that the effort was a part of "Moscow's longstanding desire to undermine the U.S.-led liberal democratic order."[106]

In March 2019, Special Counsel Robert S. Mueller's *Report on the Investigation into Russian Interference in the 2016 Presidential Election*[107] found that the Russian government used U.S. social media platforms extensively to influence the 2016 election in favor of Donald Trump. Facebook testified that 470 Facebook accounts controlled by the Russian Internet Research Agency (IRA)[108] made 80,000 posts between 2015 and 2017 reaching potentially 126 million persons.[109] In addition, "to reach larger audiences, the IRA purchased advertisements from Facebook that promoted IRA groups on the newsfeeds of U.S. audience members."[110] Using paid advertising tools on social media allowed Russian operatives to access Facebook's sophisticated ad-targeting services built on large repositories of American's sensitive personal information.

---

[105] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/NU2B-TDML].

[106] *Id*. at ii.

[107] ROBERT MUELLER, DEPT. OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION (2019), www.justice.gov/storage/report.pdf [https://perma.cc/YNJ6-EWLM].

[108] The Internet Research Agency is an organization of professional Internet trolls whose activities are coordinated by the Russian government. *See id.* at 4.

[109] *Id.* at 15 (citing *Social Media Influence in the 2016 U.S. Election: Hearing Before the Senate Select Committee on Intelligence*, 115th Cong. 13 (Nov. 1, 2017) (testimony of Colin Stretch, General Counsel, Facebook)).

[110] *Id*. at 25.

At the same time that Russian government was targeting American voters through U.S. social media platforms, Cambridge Analytica reportedly passed information to Russian intelligence services on its U.S. voter targeting activities via the state-owned Russian oil firm Lukoil.[111] According to Senator Feinstein, Lukoil has a formal information-sharing agreement with the Russian Federal Security Service (FSB), which is the successor to the KGB.[112] In addition, Cambridge Analytica used a Moldovan-born professor to extract 87 million Americans' Facebook data, primarily the results of an online personality questionnaire, that would form the basis of the firms psychological voter-targeting program.[113] Although the professor was associated with Cambridge University in London, he reportedly concealed the fact that he was also receiving compensation from St. Petersburg University in Russia.[114] U.K. Parliament Member Damien Collins, who led the Parliament's investigation into Cambridge Analytica, also confirmed that the same professor's data on U.S. voters was accessed from Russia.[115]

Authoritarian governments use U.S.-based social media platforms to conduct information operations not only in the United States, but also all over the world. Reporting suggests that Russia is using the same targeted misinformation on Facebook and Twitter in Africa,[116] the Middle East,[117]

[111] Cadwalladr & Graham-Harrison, *supra* note 1.
[112] Feinstein, *supra* note 16.
[113] Cadwalladr & Graham-Harrison, *supra* note 1; Issie Lapowsky, *Facebook Exposed 87 Million Users to Cambridge Analytica*, WIRED (Apr. 4, 2018), https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/ [https://perma.cc/DW2E-X57F].
[114] Cadwalladr & Graham-Harrison, *supra* note 1.
[115] *Facebook Data Gathered by Cambridge Analytica Accessed from Russia, says MP*, GUARDIAN (Jul. 18, 2018), https://www.theguardian.com/technology/2018/jul/18/facebook-data-gathered-by-cambridge-analytica-accessed-from-russia-says-mp-damian-collins [https://perma.cc/2LR2-D83Q].
[116] Davey Alba & Sheera Frenekl, *Russia Tests New Disinformation Tactics in Africa to Expand Influence*, N.Y. TIMES (Oct. 30, 2019), https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html [https://perma.cc/EF2W-Z9EP].
[117] Katherine Costello, *Russia's Use of Media and Information Operations in Turkey,* RAND CORP. (2018), https://www.rand.org/pubs/perspectives/PE278.html [https://perma.cc/UF5G-QDRT].

Latin America,[118] and the Baltic States.[119] The Senate Foreign Relations Committee found that Russian "disinformation efforts can now take advantage of increasingly powerful analytics that identify 'customer sentiment,' allowing them to target the most susceptible and vulnerable audiences."[120] The Carnegie Endowment for Peace found that prior to disbanding, Cambridge Analytica "ha[d] been active in Mexico, Brazil, and possibly Columbia, raising the specter of Russian or other external attempts to manipulate public opinion during an election year. Tipping just one or two countries toward an anti-U.S. stance—especially long-time U.S. partners—could complicate U.S. policy and distract Washington from its global priorities."[121] Finally, the Computational Research Project at Oxford University found evidence of social media manipulation campaigns in 70 countries in 2019—up from 23 in 2017; these campaigns were conducted via computational propaganda intended to shape domestic public opinion by governments or political parties.[122]

Cambridge Analytica illustrated the Russian government's direct interest in U.S. voter data. Because the Russian government sought such data—while conducting information operations targeting U.S. voters that closely resembled Cambridge Analytica's services to a U.S. Presidential candidate—there is additional evidence that Cambridge's data and or methodology achieved some level of effectiveness. That the Russian government has continued to expand the same type of operations around the world further speaks to the efficacy of these tactics.

---

[118] Julia Gurganus, *Russia: Playing a Geopolitical Game in Latin America*, CARNEGIE ENDOWMENT FOR INT'L PEACE (May 3, 2018), https://carnegieendowment.org/2018/05/03/russia-playing-geopolitical-game-in-latin-america-pub-76228 [https://perma.cc/W2FG-KVHD] ("Populations in Latin America are particularly avid social media users compared to other regions in the world, according to data collected in 2015, making them susceptible to potential Russian efforts to promote divisive or anti-U.S. narratives via online platforms.").

[119] Oliver Backes & Andrew Swab, *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States*, BELFER CTR. (Nov. 2019), https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states [https://perma.cc/NEN8-WP5E].

[120] STAFF OF THE S. COMM. ON FOREIGN RELATIONS, 115TH CONG., PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY 2 (Comm. Print 2018).

[121] Gurganus, *supra* note 118..

[122] SAMANTHA BRADSHAW & PHILLIP HOWARD, COMPUTATIONAL PROPAGANDA RESEARCH PROJECT AT THE OXFORD INTERNET INSTITUTE, THE GLOBAL DISINFORMATION ORDER: 2019 GLOBAL INVENTORY OF ORGANISED SOCIAL MEDIA MANIPULATION, (2019), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf [https://perma.cc/LQ49-5RDW].

Given the advances in the efficacy of mass persuasion techniques, powered by U.S. social media platforms and their large repositories of personal data, information operations ought to be considered a strategic level concern. They have the potential to undermine elections in the United States and in partner democracies around the world, particularly those with less developed civil societies. The Cambridge Analytica affair demonstrated that hostile nations are actively seeking sensitive U.S. voter information. As a result, the government has a clear interest in some regulation of the collection, use, and transfer of voters' personal information.

B. Rights Balancing and the Legal Argument

Even if a court were to find the factual basis supporting voter privacy compelling, that court would still be required to balance those interests against other competing rights and whether any restrictions were properly tailored to meet those interests.[123] To that end, the Voter Privacy Act provides a useful test case to consider the potential competing interests associated with regulating the use of voters' data as described in Section A, namely voters' privacy versus transparency and speech.

1. *The Voter, the Candidate, and the People*

Although courts have generally favored transparency over privacy with respect to regulating political campaigns, the Voter Privacy Act could reorient the equities underlying those decisions. In the context of campaign finance, courts have generally understood privacy as an individual right, and transparency or anticorruption as a right of the public or "the People." In *Buckley*, when describing privacy the Court uses terminology associated with the individual: "[disclosures] will deter some *individuals* who might otherwise contribute,"[124] "disclosures may even expose *contributors* to harassment or retaliation,"[125] and "not insignificant burdens on *individual* rights."[126] In contrast, when describing transparency interests, the Court uses terminology emphasizing the collective: "disclosure provides the *electorate* with

[123] *See* Sorrell v. IMS Health, Inc., 564 U.S. 552, 577 (2011) (explaining that Vermont's chosen manner of restricting speech is too burdensome); *see also* United States v. Stevens, 559 U.S. 460, 482 (2010) (holding that a content-based speech restriction was overbroad and so not properly tailored).
[124] *See* Buckley v. Valeo, 424 U.S. 1, 96 (1976) (Burger, J., concurring in part) (emphasis added) (citation omitted).
[125] *Id*. at 69 (emphasis added).
[126] *Id*. (emphasis added).

information,"[127] "exposes [corruption] to the light of *publicity*,"[128] and "a *public* armed with information about a candidate's most generous supporters."[129]

Implicit in the Court's reasoning in *Buckley* is a twofold analysis. The first is a normative judgement about transparency and privacy in elections. The second is a utilitarian balancing of the interests *of the many* in transparency versus the interests *of the few* in privacy. The Court's reasoning here appears sound; elections are about effectuating the will of the electorate.

However, the same logic yields a different result as it relates to the Voter Privacy Act. First, whereas in *Buckley* the Court considered two constituents—public and individual—the Voter Privacy Act appears to have three—voter, candidate, and the public. Classifying the interests associated with the first two is relatively straightforward. The voter has a *privacy* interest in being able to control the use of their personal information in an election, including to mitigate the increasing potential for psychological manipulation by organizations like Cambridge Analytica. The candidate has a *speech* interest in access to voters' personal information in order to communicate more persuasively with voters.

Because the Voter Privacy Act allows voters to dictate the use of their own personal information once in possession of a candidate, the inevitable conflict and the Court's analysis would likely begin with those two competing claims—voter and candidate. Unfortunately, there is no definitive instruction in *Buckley* about the relative weight of an individual voter's privacy interest versus a candidate's speech interest.

It is clear from *Sorrell* that limiting access to data is a burden on protected speech. Therefore, ordinarily whether the Court would sustain such a regulation would turn on the government's countervailing interest. However, in the case of the Voter Privacy Act, the competing interest is not the government's—it's the voter's. In the context of an election, which is a direct exercise of sovereign authority in democracy, it seems likely the Court would find the voter's interest more compelling. As described in Section A, the voter's interest is even more compelling in light of the information popularized by Cambridge Analytica: the more data that is known about a voter, the greater the likelihood of a third-party altering that voter's behavior through psychological manipulation. However, the simplest way to think about it might be: it would be an odd holding for the Court to find that a candidate seeking representative office has more of a right to voters' personal information than the voters themselves.

---

[127] *Id*. at 66 (emphasis added).
[128] *Id.* at 67 (emphasis added).
[129] *Id.* (emphasis added).

The third interest the Court would likely consider is the public or the People. In *Buckley*, the public interest was rightly aligned with transparency. The Court reasoned that though some wealthy campaign contributors would have to disclose their political contributions, the vast majority of the electorate would benefit from elections less likely to include corruption. Again, the Voter Privacy Act seems to alter that assessment.

As Dr. Priscilla Regan rightly points out, political privacy is not only an individual right, but a "*public* value that supports democratic political systems."[130] Therefore, the privacy necessary for an individual voter to exercise independent judgement in an election is not only an interest of a voter, but of all voters—and even democracy itself.

In addition, Cambridge Analytica's connection between the amount of data available about a voter and potential for psychological coercion further supports the public's interest in voter privacy. First, the public has an interest in being governed by a government that is a legitimate reflection of the People's will. Second, the public has a national security interest in mitigating the ability of foreign nations to manipulate the electorate through mass digital persuasion like the kind implemented by the Russian government, and potentially aided by Cambridge Analytica. On the other hand, there does not appear to be the same persuasive case that the public has an interest in a candidate's having unregulated access to voters' personal information, particularly over the objection of the voters themselves.

Therefore, even if the Court did not find that an individual voter's right to privacy outweighed a candidate's right to access that voter's personal information, the combination of the voter and the public's interest would be dispositive.

2. *Preserving a Candidate's Access to Data*

The second consideration is whether the Voter Privacy Act's potential limitation on access to data would undermine a candidate's ability to communicate persuasively with the electorate. In *Sorrell*, the court confirmed that access to data is protected speech[131] and that salespersons are more effective when they know the background and purchasing preferences of their clientele.[132] It is also well-established that the Court's concerns would be heightened in the context of political speech.

---

[130] PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225–27 (1995).
[131] Sorrell v. IMS Health, Inc., 564 U.S. 552, 571 (2011) ("Facts, after all, are the beginning point for much of the speech that is most essential to … conduct human affairs").
[132] *Id.*

The Voter Privacy Act includes a number of important limitations that could mitigate those concerns. Unlike the statute at issue in *Sorrell*, the Voter Privacy Act does not include an initial restriction on any voter's data. Candidates could continue to collect any type of voter data and would continue to have access to that data, absent a voter's intervention.

The Voter Privacy Act also excludes three categories of data from voter control: publicly available information, deidentified information, and aggregate polling information. Meaning, if a candidate only obtained information from state voter registration databases and anonymized polling data, she would not be subject to any voter instructions or limitations on the use of that data because it is outside the scope of the bill.

Moreover, the data contained in voter registration databases appears to be meaningful. They include significant information like name, address, signature, date of birth, phone number, gender, party affiliation, and voting history.[133] And, there is evidence that it is some of the most useful information available. According to Rubenstein, state voter registration databases "play[] a critical role in the U.S. political system by enabling candidates and others to communicate with voters for political purposes by mail, phone, email, and door-to-door canvassing."[134] Moreover, at least some academics and political professionals argue that, as of 2014, publicly-available voter registration data was the most important source of information for campaigns.[135]

The absence of blanket restrictions on voters' data coupled with the exclusion of state voter registration databases and anonymized polling data from the bill ensures candidates would have access to at least some meaningful voter data. Defenders of the legislation would likely point to these provisions as evidence that the bill is narrowly tailored; however, it is likely to also factor in the court's balancing of rights as well.

V. CONCLUSION

There may actually be more than one silver lining associated with Cambridge Analytica. The first is that this affair firmly established the challenges associated with the application of Big Data to democratic elections in the public conscience. The firm provided a road map for citizens and policy makers to consider the emerging science around Big Data and the national security risks associated with unregulated access to voters' personal information.

And, with credit to Senator Feinstein, the affair also resulted in the introduction of the first federal legislation in our history that would regulate

[133] Rubenstein, *supra* note 23, at 868.
[134] *Id.*
[135] *Id.* at 886.

the use of voters' personal data in elections. Hopefully, it will also result in courts reconsidering concepts like voter and political privacy and whether they merit increased attention in the Digital Age.