ELECTION LAW JOURNAL
Volume 19, Number 2, 2020
Mary Ann Liebert, Inc.
DOI: 10.1089/elj.2020.0633

Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity

Holly Ann Garnett and Toby S. James

ABSTRACT

Elections are essential for delivering democratic rule, in which ultimate power should reside in the citizens of a state. This introduction argues that the management and contestation of elections have now entered a qualitative new historical period because of the combined development of new technology and broader sociological developments. The era of cyber-elections is marked by: (a) the new ontological existence of the digital, (b) new flows of data and communication, (c) the rapid acceleration of pace in communications, (d) the commodification of electoral data, and (e) an expansion of actors involved in elections. These provide opportunities for state actors to incorporate technology into the electoral process to make democratic goals more realizable. But it also poses major threats to the running of elections as the activities of actors and potential mismanagement of the electoral process could undermine democratic ideals such as political equality and popular control of government. The article argues that this new era therefore requires proactive interventions into electoral law and the rewriting of international standards to keep pace with societal and technological change.

Keywords: cybersecurity, electoral integrity, ICTs, elections, democracy, electoral management

INTRODUCTION

THE USE OF NEW TECHNOLOGIES in elections has emerged as a key issue in recent years, with concerns about database hacking, media manipulation, and foreign technological interference leading to public concern and debate around the world. Recent examples make the relevance of this issue clear. The U.S. Senate Intelligence Committee found evidence of Russian interference and media manipulation in the 2016 American presidential election (United States Senate Intelligence Committee 2019a, 2019b). Estonia's widely respected identity card system, which is used for I-voting in elections and access to government services, was recently found to be susceptible to identity theft (BBC News 2017). Meanwhile, social media has opened up a new domain of political interactions, as illustrated

Holly Ann Garnett is an assistant professor in the Department of Political Science and Economics at the Royal Military College of Canada in Kingston, Ontario. Toby S. James is a professor in the School of Politics, Philosophy, Language and Communication Studies at the University of East Anglia in Norwich, United Kingdom. The authors are grateful to Alex Williams, Ben Little, and Sally Broughton-Micova for their comments on an earlier version of this article. They would also like to thank participants of the 2018 pre-American Political Science Association (APSA) workshop on "Building Better Elections: New Challenges in Electoral Management" (Boston, Massachusetts) and the 2018 workshop on "Defending Democracy: Confronting Cyber-Threats at Home and Abroad" (Ottawa, Canada).

by claims of bots trying to influence the 2016 Brexit referendum (House of Commons Digital, Culture, Media, and Sport Committee 2019; Public Administration and Constitutional Affairs Committee 2017).

While technology has been used in elections for decades in the form of electronic voting machines and digital registration databases, the explosion of new technologies and increasing access to these technologies by citizens and election administrators demands further academic consideration. This special issue considers the question: What are the impacts of new technologies on electoral integrity?

This introduction argues that elections are an essential component in the delivery of democratic rule, which requires ultimate power residing in the citizens of a state. The management and contestation of elections have now entered a qualitatively new historical period because of the combined development of new technology and broader sociological developments. The era of cyber-elections is marked by (a) the new ontological existence of the digital, (b) new flows of data and communication, (c) the rapid acceleration of pace in communications, (d) the commodification of electoral data, and (e) an expansion of actors involved in elections. These provide opportunities for state actors to incorporate technology into the electoral process to make democratic goals more realizable. But it also poses major threats to the running of elections as the activities of actors and potential mismanagement of the electoral process could undermine democratic ideals such as political equality and popular control of government. This article argues that these new technological realities of running elections require proactive interventions into electoral law and the rewriting of international standards to maintain democratic integrity.

This introduction proceeds as follows. Firstly, it considers how technology has become integrated into democratic life, throughout the electoral cycle. Next, it asks: How are elections in this new technological environment different? It then proceeds to suggest a means of evaluating electoral integrity through democratic theory, and finally applies these ideals to elections in a new digital environment. The final section concludes with an overview of the special issue to come, policy implications, and other research directions that remain to be addressed. Based on the arguments in this article and those which follow in the special issue, this introduction calls for a major reconsideration of electoral law in many polities and at the international level.

HOW HAS TECHNOLOGY BECOME INTEGRATED INTO THE ELECTORAL CYCLE?

The use of technology in elections is not necessarily new. From the advent of radio and television for campaign advertising to the adoption of computer-based technologies in local election offices, there has been a slow advance of the integration of technology into the management of elections. In recent years though, it would seem like this growth of technology in elections has exploded. Electronic voting and Internet voting often first come to mind when we think about new technology in elections, but in fact, technologies have been adopted at all stages of the management and contestation of elections, by a variety of different actors. The electoral cycle approach, used here, emphasizes that elections are events which take place on a single day.[1]

Before an election is even called, preparations are taking place: electoral laws are passed and implemented, voters are registered, and electoral management bodies (EMBs) are planning for the upcoming contest. Technology is used throughout these processes, from the simplest computer databases used to organize potential polling stations and poll workers to more complex outward-facing systems for voter registration. In fact, a variety of new technologies have been implemented in attempts to improve the voter registration system for both voters and electoral management bodies. This has included innovations such as biometric registration, where biometric data such as fingerprints are collected as part of the registration and identification process for voters (Piccolino 2016) and online registration systems which move the registration process to an online platform to be used by voters remotely (Barreto et al. 2010; Garnett 2019a). There might be complex systems of automation used to add names to the electoral register from other government data sources.

Moving into the campaign period, new technologies, particularly the Internet and social media, have brought new forms of campaigning and with that, new challenges. Voters' preferences and activities online can be captured and used for direct targeting and advertising by political parties, candidates, or third-party interest groups. In modern elections, firms collect information on voters' online activities and preferences, and then are hired by campaigns to use these

[1]For more about the electoral cycle, see <https://aceproject.org/electoral-advice/electoral-assistance/electoral-cycle>.

data to build targeted advertisements (Persily 2017). The Cambridge Analytica scandal, for example, highlighted to the world the common practice of using voters' data, often collected elsewhere, for campaigning purposes. This issue as it pertains to electoral campaigning and voter behavior is covered in other works (Bodó, Helberger, and de Vreese 2017), but this special issue is most concerned with the legal and administrative responses to these new challenges in political campaigning. Election management bodies, courts, and policymakers have had to consider the appropriate uses of these data and privacy issues relating to them, including how they relate to the regulation of campaign media and finance.

The final stages of the electoral cycle are election day and its aftermath. Here we are concerned with the process of votes being cast and counted, as well as whether these results are respected. It is first important to note that in many countries voting takes place over a series of days, either with rolling election dates (as is the case in India's elections) or with advance voting opportunities via postal or in-person early voting. But whether voting is taking place on one day, or over a series of days, online or in-person, the use of technology in the casting and counting of ballots is perhaps one of the oldest lines of inquiry regarding the use of technology in elections. Here, we tend to delineate between e-voting, which includes the use of technology at the ballot box, such as DREs (direct-recording electronic voting), where a computerized device is used for both the casting and counting of the ballot, or optical scanning machines, where the vote is cast on paper but counted with the assistance of technology; or I-voting, which involves the use of personal technology, far from any polling station, as in the case of online voting (MIT Election Data + Science Lab, n.d.). Each of these opportunities for casting and counting ballots with the assistance of technology has received some attention, as it relates to their ability to promote (or detract from) secure, accurate, accessible, and trusted elections.

THE CYBER ELECTIONS ERA: HOW CYBER ELECTIONS ARE DIFFERENT

A number of sociologists have argued that we have entered new eras of human civilization because of profound technological or other societal changes. This could be the era of the network society, the knowledge economy, the post-capitalist age, an accelerationist era, or surveillance capitalism (Castells 1996, 2000; Srnicek and Williams 2015; Webster 2014; Zuboff 2019). The challenge of running and contesting elections is not inseparable from such broader developments. Elsewhere, James (2014, 146–149) distinguishes between premodern, modern, and post-industrial digital age eras of elections within the early industrializing established democracies. New challenges arise for running elections in each era, and techniques have therefore had to adapt to avoid institutional drift.

Here, we contend that there are five clear qualitative differences about the elections in the digital era. We focus only on the impact of technology. These are not instant transformations because the emergence of the digital has been a long-running development and the transformations are also linked to broader societal processes. They are, however, worth making clear because they have major implications for how elections are run. They have broadly occurred during the post-industrial era for the early industrializing societies. But what is notable is that the era of cyber elections is a global phenomenon that has caused disruptions and opportunities across all societies at very different levels of economic and democratic development because of the simultaneous availability of these technologies (Cruz-Jesus, Oliveira, and Bacao 2018; Norris 2002).

The era of cyber elections is marked by five core characteristics. First, cyber elections are marked by the *new ontological existence of the digital*. Organizing elections has always involved the flow and storage of information by electoral management bodies, campaigners, and government agencies. Even the earliest of elections in Athenian times would have involved the storage of electoral registers and vote tabulations. However, advances in computational power have rapidly expanded the capability to increase the volume of this information, and the nature of the data has changed. This poses major opportunities for electoral authorities, but also poses challenges in the management and regulation of data. Three forms of data can be identified:

1. *Data held by EMBs.* This may have initially been limited to paper copies of names on electoral registers, structured by geographical district. The advent of computer systems gradually allowed the development of centralized digital registers with more detailed information on citizens. An increase in computational power and

connections allows the information to be more easily combined with other governmental datasets.

2. *Voter personality data.* This includes data held externally about voters by firms such as Google, social media companies, and credit reference agencies about citizens, including political preferences and consumer preferences, which can be helpful for parties wanting to micro-target voters (Moore 2018). Zuboff (2019) charts the extensive capturing of data about our behavior from our use of technologies ranging from search engines to mobile phones to household appliances. This can then be used to extrapolate personality and political inclination.
3. *Campaign information.* There is new data on social media—the content and metadata of posts and articles about the election—which was previously not available and may therefore need regulation. Chadwick (2017) describes the development of hybrid media systems which helpfully describes the transformation in the campaign environment where physical campaigning activity continues, but it is accompanied by the digital.

Second, the era of cyber elections is marked *by new information flows of data*.[2] For example, whereas electoral registers were once stored in rusty filing cabinets, which could only be accessed by those who were physically present and able to access the key, they can now be accessed around the world by those with both legitimate and illegitimate reasons for accessing them. This might include other government departments looking to undertake socio-demographic censuses of the population or to undertake immigration or social security checks of citizens. It might also include overseas actors seeking to access, manipulate, or sabotage key electoral infrastructure.

Third, the era of cyber elections is marked by the *speed of communications and data exchanges*. The digital availability of information and advances in telecommunications infrastructures means that many aspects of the electoral process can occur at a higher speed. Voter registration applications are not dependent on the postal system, but can be submitted live online. Campaign information can be sent immediately with a tweet. Attacks on election infrastructure can be launched simultaneously in multiple locations through a cyber-attack. This new speed is a major development which has been long commented on by sociologists (Castells 1996). The new speed of information transfer opens opportunities for EMBs to provide more efficient services, but may also require immediate action if false or misleading information is spread.

Fourth, there has been the *increased commodification of electoral data*. Data relating to elections have always had an instrumental importance for those responsible for running elections, and for parties and candidates. However, data such as the electoral register and political preferences of voters have taken on a new monetary value. The electoral register is often used for purposes beyond running elections such as enabling the credit reference checking of citizens. Multinational companies therefore purchase localized registers to create new centralized datasets, which are then used to generate profit (James and Bernal 2020, 24–27). More famously, companies such as Cambridge Analytica have harvested personal information from millions of users in order to advise campaigning teams for monetary gain (Cadwalladr and Graham-Harrison 2018). Zuboff (2019) describes this as a key part of the move to surveillance capitalism.

Fifth, cyber elections are marked by *an expansion in the range of actors involved in electoral governance* who may also embark on new tactics and strategies to achieve their objectives. Elections take place in a "constellation of actors involved in steering and delivering elections, including the micro anthropological practices, beliefs and power relationships between them" (James 2020, 270). These might traditionally involve EMBs that are responsible for organizing the election, the governments and legislatures/legislators who set the rules for how elections are run, and the political parties and candidates who are seeking to run in the election. They also include media outlets that play a crucial role in disseminating information to citizens about the electoral process, democracy, and the parties and candidates. Civil society groups can help boost voter turnout through registration campaigns or providing political support for candidates.

The move towards cyber elections in a digital age can have different implications for each set of actors. For EMBs, technology presents new means

[2]We are grateful to Alex Williams for this point.

with which to deliver elections that could improve the citizens' experience or make back-office processes more economically efficient. For parties and candidates, they provide new opportunities to campaign. The digital domain is a new area through which information can be spread that might not be regulated in the same way as other aspects of the electoral process. There are opportunities for new media outlets to emerge with different business models. Civil society groups can quickly mobilize citizens through social media channels.

But at the same time new actors come into the electoral scene. Social media companies have new powers to shape the information that citizens see, develop behavioral nudges, and set policies that could shape elections worldwide. The volume of "media outlets" has expanded with anyone worldwide able to set up a website and create content about an election. External state actors are also suddenly able to orchestrate misinformation campaigns or propaganda in support of candidates or parties worldwide with ease, because it does not require the physical deployment of personnel or information to a polity. The range of suppliers of equipment also expands as companies worldwide seek to gain new market shares of the technology used in electoral management, from databases to electronic voting machines, albeit partly as a result of globalized and deregulated information and communication technologies (ICT) markets and shifts by governments to use new public management policies. There are also new entrepreneurial private sector companies seeking to extract profit from electoral data.

HOW CAN WE EVALUATE ELECTORAL INTEGRITY IN THIS CONTEXT?

The new era can lead to major shifts in power as actors have new strategies and tactics available to them. In order to evaluate the impact of the new age of cyber elections on electoral integrity, it is first necessary to better define the principles of electoral integrity, drawing first on democratic theory.[3] At their core, elections must be considered in terms of their role in delivering democracy as a political system. Democracy is simplistically thought of as "rule by the people." It can therefore be juxtaposed with other "-cracies" such as autocracies, plutocracies, and stratocracies, in which the power resides with the landed nobility, wealthy, or military. Democracy is therefore the political system which many countries reached following historical struggles against aristocratic elites, rich landowners, or authoritarian leaders. This power is, of course, exercised through representatives on their behalf, with elections providing the mechanism for the selection of those representatives.[4]

A parallel development in the process of democratization was the development of the state system. "The people," in the post-Westphalian era, are those identified as citizens within nationally bounded, hermetically sealed polities (Axtmann 2004). There are sometimes voting rights for citizens living overseas, or resident citizens of other nationalities. But in this regard, there should therefore be no influence for external governments, companies, and citizens.

There have been attempts to define democracy in more detail. Robert Dahl famously provided a minimalist concept of it as "the continuing responsiveness of the government to the preferences of its citizens, considered as political equals" (Dahl 1971, 2). David Beetham (1994), meanwhile, saw democracy as the fulfillment of key principles including the realization of political equality and popular control of government. In all definitions, however, elections remain the crucial instrument for achieving democracy. They are not the only instrument. Others such as open and accountable government and civil and political rights are all also required. Nonetheless, elections enable the peaceful transition of power and enable citizens to gain democratic representation and to hold governments to account. We argue that there are three principles that are necessary for democracy; all three could be affected by the deployment of technology.

One is the importance of *opportunities for deliberation*. Citizens need, as Dahl put it, full opportunities to formulate their preferences (Dahl 1971, 2–3). This means freedom to form and join organizations, freedom of expression, the right to vote, the right to compete for public office, and alternative forms of information. Less minimalist approaches require active deliberation of information and issues

[3]For a discussion of alternative conceptualizations see Norris (2014, 21–39) and of electoral management quality see James (2020, 33–86).

[4]There are also many variants of democracy such as liberal democracy, social democracy, consociationalist and majoritarian democracy, which all present different demands on elections. They all have elections as an essential component, however.

by citizens (Fleuß and Helbig 2020). Simply holding elections is insufficient since there is no guarantee that citizens will actively consider their interests and the issues—or that they will vote. There is therefore the risk that elections could be taking place within a "zombie democracy" of apathy and disengagement (Koch 2017).

A second principle that should underpin elections is *equality of participation*. Political equality is central to the practice of elections. Historically, polities are deep in social and economic equality, but there should be political equality. Any given polity might have economic inequality, but there should be political equality between citizens. One major threat to this equality has been the turnout gap, in which there are differential levels of participation by groups, whether by age, ethnicity, educational level, socioeconomic status, or otherwise. The proposed solution to this is the use of inclusive voting practices which seek to redress this turnout inequality and other forms of inequality in the electoral process (James and Garnett 2020). Technology, here, could be a game changer in providing new opportunities and threats to meet this principle, and what constitutes an inclusive voting practice.

A third principle is *robust electoral management quality*. Electoral laws can be designed in ways which support and strengthen democracy, but like all public policies, they require successful implementation on the ground. The PROSeS framework sets out a range of principles which are important for realizing broader democratic goals (James 2020). The service that is provided to the voter and that she should expect is not unlike that of schools or hospitals. Convenience, quality of service, transparency, professionalism, probity, cost effectiveness, and citizen and stakeholder satisfaction are all hallmarks of good equality election delivery, just as they are for other public services. These are important principles in their own right, but can also have instrumental effects. Long queues at polling stations, for example, can undermine voter confidence in the electoral process (King 2019). We know that public confidence in elections is crucial for democratic legitimacy (Lipset 1960; Norris 2014). If citizens believe that their votes have created the government, they will be more likely to perceive it as legitimate. However, if citizens believe that an election was manipulated, they will have less reason to see it as legitimate. The consequences of a loss in democratic legitimacy can range from protests and civil disobedience, to violent conflicts or the election of anti-establishment populist leaders, and even the collapse of democracy (Norris 2014). As such, any implications of technology for the management of elections, including how this management is perceived, is crucial.

These three principles are not necessarily exhaustive but do present some essential elements of electoral integrity to ensure democratic rule. Importantly, they are all dependent on electoral law. Election law is a crucial consideration in delivering these key principles because it specifies the rules of the game, regulates proper roles, and structures power relations within systems of electoral governance. At the international level, international legal and nonbinding agreements are important because they can norm-set the appropriate behavior of actors (Hyde 2011). For example, the United Nations International Covenant for Civil and Political Rights (1966) states that all citizens have the right "to vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors."[5] Rapid developments, however, including the introduction and increase of digital technology, require that electoral law and practices be changed so that electoral integrity can be achieved in this new environment. This may involve changing or updating laws and regulatory regimes within national polities, but also a reconsideration of whether the international standards that were defined as "best practice" for elections are fit for purpose or in need of revision themselves, if we want to realize democratic objectives. For this reason, those international "best practices" cannot provide an anchoring definition of electoral integrity since they need to respond to changed circumstances.

[5]Article 25, Section B of the United Nations International Covenant for Civil and Political Rights (1966) (<http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>). See also an earlier document, the United Nations Universal Declaration of Human Rights (1948) (<http://www.un.org/en/universal-declaration-human-rights/>). Other examples include United Nations Convention on the Political Rights of Women (1952) (<http://www.un.org/womenwatch/directory/convention_political_rights_of_women_10741.htm>); Organization for Security and Cooperation in Europe Copenhagen Document (1990) (<http://www.osce.org/odihr/elections/14304>); and Inter-Parliamentary Union Declaration on Criteria for Free and Fair Elections (1994) (<http://www.ipu.org/cnl-e/154-free.htm>).

HOW ARE THESE IDEALS ACHIEVED OR THWARTED IN A NEW TECHNOLOGICAL ENVIRONMENT?

We therefore ask: How can these democratic ideals of electoral integrity be achieved or prevented in a new technological environment? What new strategies or tactics are available to actors? What responses and changes in laws, practices, and agreements may be necessary to respond to this new environment? The articles in this special issue explore these questions, tackling a variety of technologies, geographic cases, and stages of the electoral cycle. To begin this conversation, however, we consider the three major principles of electoral integrity mentioned above—the opportunity for public deliberation, the equality of participation, and finally, the professionalism and impartiality of the delivery of elections as a public service—and how they may be helped or hindered through the use of technology in elections.

Deliberative opportunities

In order for elections to be robust public exercises of deliberation and decision, the debates and discussion must allow for widespread participation, and the provision of adequate information for citizens to make a decision and get to the polls. How have new technologies in the digital age impacted the integrity of this public deliberation and discourse?

It is not surprising that technology, especially in the form of social media, may help broaden avenues for deliberation, with new means of debating and discussing ideas and gaining political knowledge. The Internet, let loose, allows the immediate and freer exchange of information that can facilitate deliberation. However, there are also particular challenges that have been brought to light in recent years. One challenge regarding the use of social media to advertise issues and candidates during elections is the inequality of information. With direct targeting on social media in particular, candidates and campaigns can tailor their messages to specific groups of voters, down to very specific variables. While this may be effective for candidates, it can also contribute to the creation of an "echo chamber," where voters only hear the sorts of messages that campaigners think they will be receptive to (Barberá et al. 2015). This can contribute to polarization of the electorate and national politics (Baum and Groeling 2008; Gruzd and Roy 2014).

Additionally, this may lead to some new forms of inequality in the campaign since different voters are hearing different messages. This may inhibit the ability of all voters to consider the same messages and issues when deciding whom they will vote for. This is challenging especially in larger or more diverse countries, since issues that unite the country may not be considered in election campaigns.

Relating to the types of messages that voters are likely to hear during a campaign, we now turn to perhaps the most well-known issue regarding the cyber-threats to elections: namely, the threat of disinformation, or the deliberate dissemination of incorrect information to sway public opinion and/or political behavior, a phenomenon observed in many regions of the world (Bradshaw 2018; Education for Justice 2019; Funk 2019; Guest Blogger 2019).

Disinformation campaigns can target a variety of electoral actors. Electoral management bodies fear disinformation about electoral procedures or results. This is not a new phenomenon. For example, Canada's "robo-calls" scandal in the 2011 federal election saw voters nefariously misled about their polling locations via automated telephone calls on election day (Pal 2017). However, the ability for information to spread via social media makes this threat particularly dangerous. If a malicious actor was able to access an EMB's website or social media account, for example, they could easily provide false information or fake election results. Ghana's 2016 presidential election, for example, faced both the hacking of their website and misinformation on the results spread throughout social media, prompting the EMB to tweet for voters to ignore the results that were circulating (BBC News 2016).

Likewise, we have seen numerous examples of the types of information that voters receive about their candidates being manipulated or falsified and distributed via online media. Examples include impersonation of candidates' social media profiles, which can then provide false messaging or information to voters (Garnett et al. 2019). Another new challenge is so-called "deep fakes," or videos or photos that have been doctored to provide false information. Even if these types of disinformation are detected and corrected, the damage may already have been done in the minds of voters.

Another issue that must be addressed is the potential for harmful speech online, including intimidation, violence, and threats, that are less easy to trace and protect from (Brown 2017). This may

influence who is willing to participate in politics, if past social media usage, or future threats, are taken into consideration when deciding to run for office (Tenove, Tworek, and McKelvey 2018). Some research on the impact of online campaigning, for example, has considered its effect on the participation of women in elections. Bardall (2013) has documented the rise of violence against women in elections via new technologies. Bardall (2013) explains that a woman's public image may be easily degraded, they may be intimidated, or may disproportionately be the target of direct attacks, silencing, or media bias. However, she also acknowledges that new technologies can likewise facilitate the monitoring and documentation of violence against women and be a key tool of female empowerment when used appropriately.

A further implication of new media is on the balance of power between candidates and parties competing for office. During the course of the twentieth century there was a move to tighten the regulation of election campaigns to restrict the amount of money that could be spent by candidates and parties (Norris and van Es 2016). This was partly borne from a concern that those who had the most financial resources could use these to influence voters and would therefore have an unfair advantage at election time. The era of cyber elections, however, meant that regulations and laws restricting physical campaigning do not necessarily apply to online campaigning. Financiers are more readily able to give unrestricted capital to parties and candidates. Party machines are able to push new content onto social media platforms and micro-target individual voters (Moore 2018). Social media platforms have new powers available to them to set algorithms, leading to concerns that there might be an algocracy (Danaher 2016). New forms of inequality in the electoral process are therefore opened up because while there might not be immediate restrictions on deliberation, the environment in which this deliberation takes place might be systematically biased towards particular candidates, thereby undermining the principle of political equality.

Equality of participation

For democratic ideals to be achieved, all citizens must be able to vote, and have their vote count equally. This issue is important even before election day, as voters are registered and resources are allocated for polling stations. Different technological means have been tested to improve the quality of registration lists. These lists are key for voters to be able to easily vote on election day, and even if pre-registration is not mandatory, voters who are registered still benefit from information mailed to them in advance of the election. Furthermore, election administrators will allocate more appropriate resources to certain areas if they have a better idea of how many voters live there.

Some of the means that have been used to improve the accessibility and accuracy of voter registration include biometric technology and online registration. In some countries, biometric data, such as a fingerprint, is now used to assist in confirming the identity of a voter. This was heralded as a key step forward in some contexts where reliable registries of all voters were not available. The idea is that it would help ensure the integrity of citizen participation since no voter could register or vote twice. However, in some cases, the use of this technology proved disastrous when it was implemented where adequate electricity and network access were unavailable (Piccolino 2016).

In other countries, rather than changing the basis of identity verification for voter registration, the means by which voters could register were changed in an attempt to make it more convenient for the voter. This includes the use of electronic voter registration done in-person and remote online voter registration systems. The latter has been adopted by many countries and provides voters the opportunity to register or amend their registration entirely online (Barreto et al. 2010; Garnett 2019a). It is thought to improve the accuracy of information since voters can amend their details when necessary (such as a change in address), and there are fewer chances for clerical errors or missing records. Some research has also suggested it may attract citizens who do not normally vote to register, such as young people (Garnett 2019a). In this way, the use of technology may improve the participation levels of under-represented population groups.

Additionally, in-person voting technology has assisted in promoting more inclusive voting. Electronic voting machines, for example, may improve accessibility, especially for traditionally under-represented voters, including minorities and those with disabilities. For example, in one case studied in Australia, e-voting was piloted as a solution to language barriers among the indigenous population

(Hill and Alport 2007). DRE-voting can also come with additional accessibility features for those with any number of disabilities, such as audio assistance, magnification for those with low vision, or adaptability for sip-and-puff devices used by some quadriplegics, to name just a few (Cross et al. 2009). They can also provide voters with disabilities the opportunity to independently cast their ballot, rather than relying on assistance from a poll worker or other assistant. Online voting may likewise improve accessibility by attracting a different population group that may not normally be able to attend a physical polling station due to any number of physical or psychological limitations.

However, technologies that may facilitate the participation of some groups may, at the same time, decrease the likelihood of others participating. Here we may find some voters beginning to distrust elections or even refusing to participate as more technology is adopted. They may see security issues that infringe upon the privacy of their personal information and vote. Whether these issues are real or imagined, they have the same effect of potentially turning some people off the voting process.

These security issues are commonly discussed in academic literature and the media. Commentators and academics alike have warned about the potential for security breaches, threatening the privacy of an individual's vote, or erasing or amending election results (Gritzalis 2003). These sets of security concerns are different for in-person technology used to cast ballots when compared with online voting. For the in-person use of technology, such as DREs, the fear is less about direct hacking, since the devices are rarely connected to the Internet, but instead the possibility that the equipment could be tampered with before the device is deployed to a polling station. Fears that electronic counting devices could be tampered with led, for example, the Dutch 2017 election ballots to be counted entirely by hand in a last-minute decision to ensure security (Chan 2017). Some security mechanisms, like paper trails and post-election audits, however, have been suggested as means to combat these security concerns associated with the use of technology at the ballot box (Burton, Culnane, and Schneider 2016; Dunn and Merkle 2018).

Online voting, of course, comes with another set of security concerns, since it necessarily involves the Internet (Hall and Alvarez 2008). This voting system may therefore be more prone to hacking to erase or amend results, or invade voters' privacy. Voters could also easily be misled by fake information about online voting, or false URLs, which, if followed, would not actually record their ballot, or could even lead to further cybersecurity breaches. Similarly, the use of technology in registration and voting may cause problems that actually prevent some voters from casting a ballot. For example, online voting could also easily be disrupted by deliberate malicious denial of service attacks, as well as simply an oversaturation of the website by legitimate voters. This was, for example, the case in many Ontario municipalities during the 2018 municipal elections, where the online voting website crashed due to technical glitches and a high volume of legitimate voters (Britneff 2018; Gollom 2018). Finally, since online voting is unsupervised, it is easy to envisage scenarios where a voter may be directly influenced or intimidated into voting a certain way, or where their privacy is infringed upon (Essex 2016).

Adding to these issues are studies linking the use of technology in voting and lower public trust. Some preliminary evidence has demonstrated that public trust can be eroded by the use of technology in elections (Alvarez et al. 2013; Alvarez, Katz, and Pomares 2011; Delis et al. 2014; Pomares, Levin, and Alvarez 2014). Voters may distrust the faceless technology of electronic voting and be concerned about whether their vote will actually be counted as intended when swallowed into the "black box" of a voting machine (Alvarez, Hall, and Llewellyn 2008; Garnett and Simpson 2019). For this reason, Card and Moretti (2007) argue, for example, that e-voting at the polls may depress turnout if not accompanied by education campaigns. Further studies have considered the relationship between online voting and turnout, though the results are mixed, with some studies showing no effect (Germann and Serdült 2017) and others suggesting it actually attracts population groups that are likely to vote anyway (Bochsler 2009, 2010).

A further threat to equality of participation is posed by digital voter suppression. Voter suppression has been a long-standing tactic of many elections. Opposition voters can be deliberately targeted with inaccurate information about the location of polling stations, eligibility requirements, or have their registration status contested (Piven, Minnite, and Groarke 2009). The era of cyber elections facilitates this suppression through the micro-targeting of particular

groups. This might include calls to boycott the election through tweets or voter intimidation, as identified in the American case (Mie Kim 2018). For some scholars, even positive micro-targeting, when using the Internet to contact and encourage certain types of voters to go to the polls, puts other voters at a disadvantage with less information about the electoral process, thus reducing their turnout (Ross and Spencer 2019).

Electoral management delivery

Finally, we consider the implications of technology for the professional, impartial, and transparent management of elections. The case of the 2000 election in the United States was a landmark example of a shift towards electronic voting mechanisms when it became clear that lever and punch-card voting mechanisms were not necessarily recording the voter's intention correctly (Card and Moretti 2007). In this case, electronic voting (DREs) was a solution to this problem, allowing voters to confirm their selection. Additionally, DREs were associated with a reduced number of residual votes, as the machines could immediately notify voters of errors, such as over-voting (Allers and Kooreman 2008; Hammer et al. 2010). Outside of the American case, electronic voting has also solved some accuracy issues, for example, in Kenya, where e-voting was a solution to an inaccurate voter register and difficulties transporting votes from polling stations to the locations where the ballots would be counted (Barkan 2013). Thus, where the security of e-voting is ensured, the process may actually allow for more accurate results.

Particularly in new democracies, the use of technology can help improve perceptions that the vote count is not being tampered with by electoral officials, since it provides a level of technological oversight and transparency, and is less easily tampered with. For example, a novel experiment in Uganda demonstrated that electoral officials who thought some technology would be used to verify their activities were more likely to comply with official count procedures (Callen et al. 2016).

There are also some opportunities associated with improving accuracy of information collected by election management bodies with the help of new technologies. For example, online registration is suggested to improve the accuracy of registration data for election management bodies. It may attract a greater portion of the population, especially population groups that may not have previously been registered, because it is more accessible (Garnett 2019a). There is also less of a risk of voters making errors, since electronic registration programs can automatically detect them. It may also reduce transcription errors (Shaw, Ansolabehere, and Stewart 2015). The use of optical scans or direct-recording voting machines on election day can likewise help to address the human error associated with hand-counted ballots. Furthermore, the advent of digital technologies can improve the spread of information, allowing electoral management bodies to contact voters in new ways to share information about voting procedures, or provide additional layers of transparency about electoral results.

The use of digital technologies may also solve some security challenges associated with protecting election data. For example, the centralization of voter registration records in a digital format can protect against the mishandling of paper files (Shaw, Ansolabehere, and Stewart 2015). It may also provide additional opportunities for the back-up of files, if they are stored via various means, as is the case for electronic voting machines with paper trails.

Meanwhile, technology has also provided opportunities for cost savings. Internet voting has been found to be the most cost-efficient way of delivering elections (Krimmer, Duenas-Cid, and Krivonosova 2020). The use of data-mining techniques to automatically reregister citizens which other public data sources suggest are still resident is thought to have led to major savings (James and Bernal 2020).

However, there are also several threats associated with accuracy in the use of technology in elections, particularly as it pertains to the accuracy of information that voters are receiving about candidates, parties, electoral events, the voting process, and even election results. Disinformation or misinformation has become a popular field of study in the social media age, where information can be disseminated quickly and prolifically without the traditional gatekeepers of the traditional media (Marwick and Lewis 2017). Furthermore, more actors can be involved in sharing potentially false information, since the Internet does not know the physical boundaries that once limited the spread of information.

With new technologies in elections come new security concerns. Some cybersecurity threats are

obvious, such as hacking compromising private information, such as voter registration rolls or election results. This information can then be sold, ransomed, or otherwise compromised (Buchanan and Sulmeyer 2016; National Academies of Sciences et al. 2018). This threat brings with it serious questions about the privacy of voters' data, but also their future willingness to provide information to legitimate authorities, if they fear that it may be compromised. For example, online voter registration systems can sometimes bring with them concerns about the privacy of data, and may then impact a voter's decision of whether to register to vote or not (Barreto et al. 2010).

In recent years, the distributed denial of service attack, which floods a website or service in order to render it unusable for legitimate users, has become a threat to elections (Canadian Communications Security Establishment 2017; National Academies of Sciences et al. 2018). There are already examples of this occurring in electoral contests, including perhaps the 2016 Brexit referendum, where the voter registration website crashed, and a targeted distributed denial of service was not ruled out as a potential reason why the site was temporarily unavailable (Public Administration and Constitutional Affairs Committee 2017).

All of these issues may have implications for overall trust in electoral management, and electoral integrity and democracy more broadly, which we know from previous research are related, especially in contexts where electoral integrity is fragile (Garnett 2019b). Thus, any implications of the use of technology for public perceptions of the transparency and impartiality of electoral management are key to electoral integrity.

RESPONDING WITH ELECTORAL LAW

What then are the policy consequences of entering the era of cyber elections? How can election law respond to these new challenges? Figure 1 summarizes the theoretical framework outlined in this introduction, depicting a conceptualization of how technological change has impacted elections. In the left-hand column, the major infrastructural changes are detailed. Technology, however, does not directly cause societal change—rather it opens up new strategies and tactics for actors to undertake. These strategies might be deployment of new databases of electoral registers, digital (dis)information campaigns, or other schemes described in this section. If adopted, there might be consequences for the integrity of elections and the realization of democratic ideals. The major practical question that follows, then, is what laws should be adopted to respond to these challenges? This is a research agenda that has already begun, but we hope that this special issue and the articles within it further reignite that agenda.

In the first section of this special issue, the authors considered comparative lessons and case studies into the adoption of new technologies into the electoral process, largely from an electoral management perspective. The key take-aways from these works emphasize the need for further regulation of the use of technology in elections. Key questions must be resolved at both the national and subnational levels. The major issue clarified by articles by Leontine Loeber, as well as Aleksander Essex and Nicole Goodman, in this issue is that electoral policies can sometimes be silent on major issues relating to the adoption, ownership, and contingency planning for electoral technology. Key questions that we identify include:

1. What technology can be used?
2. Who owns the technology (and resulting data)?
3. What procedures are in place if technology breaks or is faulty?

Evidence from the Ontario case presented by Essex and Goodman, as well as discussions regarding contingency planning in the United States by Mitchell Brown, Kathleen Hale, Robert J. Smith, and Lindsey Forson in this issue, highlight the need to think through these potential challenges as early as possible.

Likewise, the second set of articles calls for greater consideration of legal apparatuses to detect actions on new online media that may compromise democratic ideas, including false statements and disinformation. The challenge is to identify laws that can protect democratic space, while also protecting freedom of speech. Netina Tan's overview of various approaches from Southeast Asia in this issue suggests that further research is needed to uncover the most effective means of negotiating this delicate balance in the legal sphere.

Finally, we argue that international legal frameworks and the norms and standards that govern

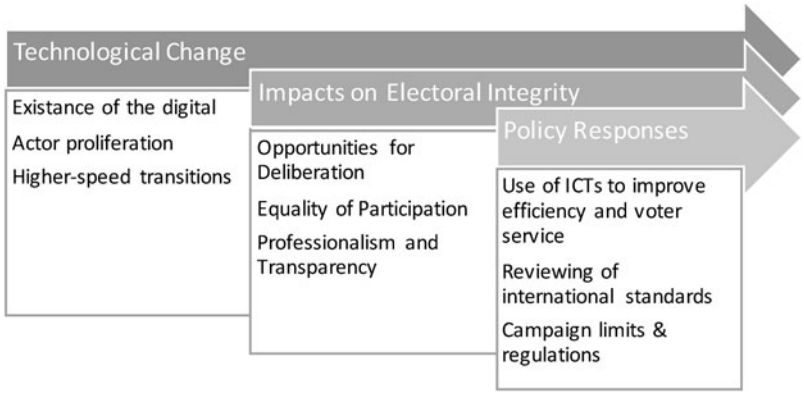

FIG. 1. Conceptualizing cyber elections and identifying policy solutions. ICTs, information and communication technologies.

elections must be adapted to cyber elections. Many of these frameworks used to commonly evaluate electoral integrity were adopted before the advent of new technologies, and the new actors and increasing speed that come with this. Electoral integrity now must include the cyber-sphere, specifically how it impacts opportunities for deliberation, the quality of participation, and the professionalism and transparency of electoral management.

In sum, election law plays a vital role in this both at the national, subnational, and international level. It may require the revisiting of international standards and handbooks. This special issue takes a major step towards considering these changes in a comparative light.

THE ISSUE AHEAD

This special issue tackles some of these emerging issues related to the use of technology in elections by focusing on two major themes: the use of technologies in electoral management activities, including casting and counting ballots, and the use of new medias for campaigning and information dissemination.

First, Loeber considers the supply, management, and governance of election technology, using new data from an international survey of electoral management bodies. It specifically looks at the ownership and control of a variety of election technologies that are in use around the globe, considering how this may impact the independence and impartiality of electoral management more broadly. Next, Ziaul Haque and David Carroll also consider the use of technologies in elections cross-nationally, considering their direct impact on expert perceptions of electoral integrity in four areas: voter registration, voter identification, election result processing, and publication of results.

This is followed by two case studies of the use of technology in electoral systems. Essex and Goodman consider online voting in Canadian municipalities, calling for actionable operational, technical, and legal guidelines for the use of online voting technologies. Brown et al., on the other hand, look at whether American election administrators provide appropriate training, resources, and assistance in their security planning and operations.

The second set of articles in this special issue looks more specifically at information and campaigning, starting with two case studies from the Canadian context. In their article on disinformation and digital information equality, Elizabeth Judge and Amir Korhani identify the Canadian legislative and judicial responses to the challenge of false statements made during elections. Michael Pal follows with an article on the use of social media, outlining the various approaches that have been taken to protect electoral integrity in the online sphere. Finally, Tan explores the challenges surrounding social media and disinformation in Southeast Asia. Her article presents a new typology of digital policy formulation and enforcement approaches, and then assesses their potential impacts on electoral integrity.

The articles in this special issue provide analysis of both cross-national and country-specific responses to the opportunities and threats brought by new technologies into the electoral sphere. Their findings highlight the diversity of responses to new technologies from legislatures, courts, and election administrators, including issues of ownership, implementation, and regulation. They highlight how these decisions can

impact electoral integrity and the quality of democracy more generally, and suggest avenues forward in the new research field of cyber elections.

Elections are entering a new digital era in which there are new opportunities and threats for the conduct and contestation of elections. Although many of these are not entirely new—perhaps being a continuation of older problems there has been a qualitative leap in the nature of the challenges. Having made this argument, this opening article has set out some criteria for evaluating the impacts of digital technology on elections and has begun to trace what effects it has had. It has focused attention on what electoral law reform should be required, within national polities, or worldwide, to address these problems. Subsequent articles in the special issue take this agenda forward.

In sum, we argue that elections are essential to democratic rule. However, our evaluations of electoral integrity require a new focus in the cyber era, with its expansion of actors, transition, and challenges in running elections. We argue that interventions to electoral law and new international standards are needed to confront these challenges and safeguard the integrity of elections.

REFERENCES

ACE. (2020). "Electoral Cycle." *ACE Electoral Knowledge Network*. <https://aceproject.org/electoral-advice/electoral-assistance/electoral-cycle>.

Allers, M. A., and P. Kooreman. (2008). "More Evidence of the Effects of Voting Technology on Election Outcomes." *Public Choice* 139: 159–170. doi: 10.1007/s11127-008-9386-7.

Alvarez, R. M., T. Hall, and M. Llewellyn. (2008). "Are Americans Confident Their Ballots Are Counted?" *Journal of Politics* 70(3): 754–766.

Alvarez, R. M., I. Levin, J. Pomares, and M. Leiras. (2013). "Voting Made Safe and Easy: The Impact of E-voting on Citizen Perceptions." *Political Science Research and Methods* 1(1): 117–137.

Alvarez, R. M., G. Katz, and J. Pomares. (2011). "The Impact of New Technologies on Voter Confidence in Latin America: Evidence from E-Voting Experiments in Argentina and Colombia." *Journal of Information Technology & Politics* 8(2): 199–217.

Axtmann, R. (2004). "The State of the State: The Model of the Modern State and Its Contemporary Transformation." *International Political Science Review* 25(3): 259–279.

Barberá, P., J. T. Jost, J. Nagler, J. A. Tucker, and R. Bonneau. (2015). "Tweeting From Left to Right: Is Online Political Communication More Than an Echo Chamber?" *Psychological Science* 26(10): 1531–1542. doi:10.1177/0956797615594620.

Bardall, G. (2013). "Gender-Specific Election Violence: The Role of Information and Communication Technologies." *Stability: International Journal of Security & Development* 3(2): 60. doi: 10.5334/sta.cs.

Barkan, J. D. (2013). "Kenya's 2013 Elections: Technology Is Not Democracy." *Journal of Democracy* 24(3): 156–165. doi: 10.1353/jod.2013.0046.

Barreto, M. A., B. Glaser, K. MacDonald, L. Collingwood, F. Pedraza, and B. Pump. (2010). *Online Voter Registration Systems in Arizona and Washington: Evaluating Usage, Public Confidence and Impelmentation Processes*. Joint research project of the Washington Institute of the Study of Ethnicity and Race (University of Washington, Seattle) and the Election Administration Research Center (University of California, Berkeley).

Baum, M. A., and T. Groeling. (2008). "New Media and the Polarization of American Political Discourse." *Political Communication* 25(4): 345–365. doi:10.1080/10584600802426965.

BBC News. (2016). "Ghana Election Commission Website Hit by Cyber Attack." *BBC*. December 8. Retrieved from <https://www.bbc.com/news/world-africa-38247987>.

BBC News. (2017). "Security Flaw Forces Estonia ID 'Lockdown.'" *BBC*. November 3. Retrieved from <https://www.bbc.com/news/technology-41858583>.

Beetham, D. (1994). "Key Principles and Indicies for a Democratic Audit." In D. Beetham (Ed.), *Defining Democracy*, 25–43. London: Sage.

Bochsler, D. (2009). "Can the Internet Increase Political Participation? An Analysis of Remote Electronic Voting's Effect on Turnout." Paper presented at the APSA 2009 Annual Meeting, Toronto, Ontario, Canada. Retrieved from: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1456827>.

Bochsler, D. (2010). "Can Internet Voting Increase Political Participation? Remote Electronic Voting and Turnout in the Estonian 2007 Parliamentary Elections." Paper presented at the Internet and Voting, Fiesole, Italy. Retrieved from <https://www.semanticscholar.org/paper/Remote-electronic-voting-and-turnout-in-the-2007-Bochsler/c3fb73248e4d8c2dadbc7aa6fcd5b1e470467364>.

Bodó, B., N. Helberger, and C. H. de Vreese. (2017). "Political Micro-Targeting: A Manchurian Candidate or Just a Dark Horse?" *Internet Policy Review* 6(4).

Bradshaw, S. (2018). "Securing Canadian Elections: Disinformation, Computational Propaganda, Targeted Advertising and What to Expect in 2019." *Behind the Headlines* 66(3): 1–13.

Britneff, B. (2018). "Online Voting in 51 Ontario Municipalities Marred by Election-Day 'System Load Issue.'" *Global News*. October 23. Retrieved from <https://globalnews.ca/news/4585577/ontario-voting-issues/>.

Brown, A. (2017). "What Is So Special About Online (as Compared to Offline) Hate Speech?" *Ethnicities* 18(3): 297–326. doi:10.1177/1468796817709846.

Buchanan, B., and M. Sulmeyer. (2016). "Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity." *Belfer Center*. October. Retrieved from <https://www.belfercenter.org/publication/hacking-chads-motivations-threats-and-effects-electoral-insecurity>.

Burton, C., Culnane, C., and S. Schneider. (2016). "vVote: Verifable Electronic Voting in Practice." *IEEE Security & Privacy* 14(4): 64–73. doi: 10.1109/MSP.2016.69.

Cadwalladr, C., and E. Graham-Harrison. (2018). "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*. March 17.

Callen, M., C. C. Gibson, D. F. Jung, and J. D. Long. (2016). "Improving Electoral Integrity with Information and Communications Technology." *Journal of Experimental Political Science* 3(1): 4–17. doi: 10.1017/XPS.2015.14.

Canadian Communications Security Establishment. (2017). *Cyber-Threats to Canada's Democratic Process*. Ottawa: Candian Centre for Cyber Security. Retrieved from <https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process/page2>.

Card, D., and E. Moretti. (2007). "Does Voting Technology Affect Election Outcomes? Touch-Screen Voting and the 2004 Presidential Election." *Review of Economics and Statitistics* 89(4): 660–673.

Castells, M. (1996). *The Rise of the Network Society: The Information Age, Economy, Society and Culture*. Oxford: Blackwell.

Castells, M. (2000). "Materials for an Explanatory Theory of the Network Society." *British Journal of Sociology* 51(1): 5–24.

Chadwick, A. (2017). *The Hybrid Media System: Politics and Power*. Oxford: Oxford University Press.

Chan, S. (2017). "Fearful of Hacking, Dutch Will Count Ballots by Hand." *New York Times*. February 1. Retrieved from <https://www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html>.

Cross, E. V., S. Dawkins, J. McClendon, T. Sullivan, G. Rogers, A. Erete, and J. E. Gilbert. (2009). "Everyone Counts: Voting Accessibility." In Stephanidis C. (Ed.), *Universal Access in Human-Computer Interaction: Applications and Services*. Lecture Notes in Computer Science, vol. 5616. Berlin and Heidelberg: Springer.

Cruz-Jesus, F., T. Oliveira, and F. Bacao. (2018). "The Global Digital Divide: Evidence and Drivers." *Journal of Global Information Management (JGIM)* 26(2): 1–26.

Dahl, R. (1971). *Polyarchy: Participation and Opposition*. New Haven, CT: Yale University Press.

Danaher, J. (2016). "The Threat of Algocracy: Reality, Resistance and Accommodation." *Philosophy & Technology* 29(3): 245–268. doi:10.1007/s13347-015-0211-1.

Delis, A., K. Gavatha, A. Kiayias, C. Koutalakis, E. Nikolakopoulos, L. Paschos, et al. (2014). "Pressing the Button for European Elections: Verifiable E-voting and Public Attitudes Toward Internet Voting in Greece." Paper presented at the Verifying the Vote (EVOTE), 2014 6th International Conference on Electronic Voting in Lochau, Austria.

Dunn, M. H., and L. D. Merkle. (2018). *Overview of Software Security Issues in Direct-Recording Electronic Voting Machines*. Paper presented at the 13th International Conference on Cyber Warfare and Security, Washington, D.C. Retrieved from: <https://www.researchgate.net/publication/326981756_Overview_of_Software_Security_Issues_in_Direct-Recording_Electronic_Voting_Machines>.

Education for Justice. (2019). "Information Warfare, Disinformation and Electoral Fraud." *E4J University Module Series: Cybercrime.* Retrieved from <https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare–disinformation-and-electoral-fraud.html>

Essex, A. (2016). "Internet Voting in Canada: A Cyber Security Perspective." Brief submitted to the House of Commons Special Committee on Electoral Reform (Canada). Retrieved from <https://www.ourcommons.ca/Content/Committee/421/ERRE/Brief/BR8610535/br-external/EssexAleksander-e.pdf>.

Fleuß, D. and K. Helbig. (2020). "Measuring Nation States' Deliberativeness: Systematic Challenges, Methodological Pitfalls, and Strategies for Upscaling the Measurement of Deliberation." *Political Studies* Retrieved from <https://doi.org/10.1177/0032321719890817>

Funk, A. (2019). "Asia's Elections Are Plagued by Online Disinformation." *Freedom House* (blog). May 2. Retrieved from <https://freedomhouse.org/blog/asia-s-elections-are-plagued-online-disinformation>.

Garnett, H. A. (2019a). "Evaluating Online Registration: The Canadian Case." *Election Law Journal* 18(1): 78–92.

Garnett, H. A. (2019b). "On the Front Lines of Democracy: Perceptions of Electoral Officials and Democratic Elections." *Democratization* 26(8): 1399–1418. doi: 10.1080/13510347.2019.1641797.

Garnett, H. A., M. Pal, C. Leuprecht, and E. F. Judge. (2019). *Defending Democracy: Confronting Cyber-Threats to Canadian Elections*. Ottawa: CDA Institute. Retrieved from <https://cdainstitute.ca/wp-content/uploads/2019/09/Defending-Democracy-Report-FINAL-1.pdf>.

Garnett, H. A., and P. Simpson. (2019). "American Trust in Election Technology." Paper presented at the Election Sciences, Reform and Administration Conference in Philadelphia, PA.

Germann, M., and U. Serdült. (2017). "Internet Voting and Turnout: Evidence from Switzerland." *Electoral Studies* 47: 1–12. doi: 10.1016/j.electstud.2017.03.001.

Gollom, M. (2018). "Glitches Are Considered Unlikely to Curb Online Voting 'Tide' Sweeping Across Ontario." *CBC*. October 25. Retrieved from <https://www.cbc.ca/news/canada/online-voting-municipalities-ontario-1.4875457>.

Gritzalis, D. A. (Ed.). (2003). *Secure Electronic Voting*. New York: Springer. doi: 10.1007/978-1-4615-0239-5.

Gruzd, A., and J. Roy. (2014). "Investigating Political Polarization on Twitter: A Canadian Perspective." *Policy & Internet* 6(1): 28–45. doi:10.1002/1944-2866.Poi354.

Guest Blogger. (2019). "Europe's Elections: The Fight Against Disinformation." *Council on Foreign Relations* (blog). May 23. Retrieved from <https://www.cfr.org/blog/europes-elections-fight-against-disinformation>.

Hall, T., and R. M. Alvarez. (2008). "Online Voting Around the World." In M. E. Felchner (Ed.), *Voting in America Volume 3*. Westport, CT: Praeger.

Hammer, M. J., W.-H. Park, M. W. Traugott, R. G. Niemi, P. S. Herrnson, B. B. Bederson, and F. C. Conrad. (2010). "Losing Fewer Votes: The Impact of Changing Voting Systems

on Residual Votes." *Political Research Quarterly* 63(1): 129–142. doi: 10.1177/1065912908324201.

Hill, L., and K. Alport. (2007). "Reconnecting Australia's Politically Excluded: Electronic Pathways to Electoral Inclusion." *International Journal of Electronic Government Research* 4(3): 1–19. doi: 10.4018/jegr.2007100101.

House of Commons Digital, Culture, Media, and Sport Committee. (2019). *Disinformation and 'Fake News': Final Report*. Eighth Report of Session 2017–19. February 14. Retrieved from <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>.

Hyde, S. D. (2011). "Catch Us If You Can: Election Monitoring and International Norm Diffusion." *American Journal of Political Science* 55(2): 356–369.

Inter-Parliamentary Union Declaration on Criteria For Free and Fair Elections. (1994). <http://www.ipu.org/cnl-e/154-free.htm>.

James, T. S. (2014). "Electoral Management in Britain." In P. Norris, R. Frank, and F. Martínez i Coma (Eds.), *Advancing Electoral Integrity*, 135–164. New York: Oxford University Press.

James, T. S. (2020). *Comparative Electoral Management: Performance, Networks and Instruments*. London and New York: Routledge.

James, T. S., and P. Bernal. (2020). *Is It Time for Automatic Voter Registration in the UK?* York: Joesph Rowntree Reform Trust.

James, T. S., and H. A. Garnett. (2020). "Introduction: The Case for Inclusive Voting Practices." *Policy Studies* 41(2–3): 113–130. doi:10.1080/01442872.2019.1694657.

King, B. A. (2020). "Waiting to Vote: The Effect of Administrative Irregularities at Polling Locations and Voter Confidence." *Policy Studies* 41(2–3): 230–248. doi: 10.1080/01442872.2019.1694652.

Koch, I. (2017). "When Politicians Fail: Zombie Democracy and the Anthropology of Actually Existing Politics." *Sociological Review* 65(1_suppl): 105–120. doi:10.1177/0081176917693550.

Krimmer, R., D. Duenas-Cid, and I. Krivonosova. (2020). "New Methodology for Calculating Cost-Efficiency of Different Ways of Voting: Is Internet Voting Cheaper?" *Public Money & Management*, 1–10. doi:10.1080/09540962.2020.1732027.

Lipset, S. M. (1960). *The Political Man: The Social Bases of Politics*. New York: Doubleday.

Marwick, A., and R. Lewis. (2017). *Media Manipulation and Disinformation Online*. New York: Data & Society Research Institute. Retrieved from: <https://apo.org.au/sites/default/files/resource-files/2017-05/apo-nid135936.pdf>.

Mie Kim, Y. (2018). "Voter Suppression Has Gone Digital." *Brennan Center for Justice*. November 20. Retrieved from <https://www.brennancenter.org/our-work/analysis-opinion/voter-suppression-has-gone-digital>.

MIT Election Data + Science Lab. (n.d.). *Voting Technology*. Retrieved from <https://electionlab.mit.edu/research/voting-technology>.

Moore, M. (2018). *Democracy Hacked: How Technology Is Destabilising Global Politics*. London: Oneworld Publications.

National Academies of Sciences, Engineering, and Medicine; Policy and Global Affairs; Division of Engineering and Physical Sciences; Committee on Science, Technology, and Law; Computer Science and Telecommunications Board; and Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology. (2018). *Securing the Vote: Protecting American Democracy*. Washington, DC: National Academies Press. Retrieved from: <https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy>.

Norris, P. (2002). *Digital Divide? Civic Engagement, Information Poverty and the Internet Worldwide*. Cambridge: Cambridge University Press.

Norris, P. (2014). *Why Electoral Integrity Matters*. New York: Cambridge University Press.

Norris, P., and A. A. van Es. (2016). *Checkbook Elections?: Political Finance in Comparative Perspective*. Oxford: Oxford University Press.

Organization for Security and Cooperation in Europe Copenhagen Document. (1990). <http://www.osce.org/odihr/elections/14304>.

Pal, M. (2017). "Canadian Election Administration on Trial: 'Robocalls,' Opitz and Disputed Elections in the Courts." *King's Law Journal* 28(2): 324–342. doi: 10.1080/09615768.2017.1351662.

Persily, N. (2017). "The 2016 U.S. Election: Can Democracy Survive the Internet? " *Journal of Democracy* 28(2): 63–76. doi: 10.1353/jod.2017.0025.

Piccolino, G. (2016). "Infrastructural State Capacity for Democratization? Voter Registration and Identification in Côte d'Ivoire and Ghana Compared." *Democratization Democratization* 23(3): 498–519.

Piven, F. F., L. Minnite, and M. Groarke. (2009). *Keeping Down the Black Vote*. London and New York: New Press.

Pomares, J., I. Levin, and R. M. Alvarez. (2014). "Do Voters and Poll Workers Differ in Their Attitudes Toward E-voting? Evidence from the First E-election in Salta, Argentina." *USENIX Journal of Election Technology and Systems (JETS)* 2(2): 1–10.

Public Administration and Constitutional Affairs Committee. (2017). *Lessons Learned from the EU Referendum*. Retrieved from: <https://publications.parliament.uk/pa/cm201617/cmselect/cmpubadm/496/49604.htm>.

Ross, B., and D. Spencer. (2019). "Passive Voter Suppression: Campaign Mobilization and the Effective Disfranchisement of the Poor." *Northwestern University Law Review* 114(3).

Shaw, D., S. Ansolabehere, and C. Stewart. (2015). "A Brief Yet Practical Guide to Reforming U.S. Voter Registration Systems." *Election Law Journal* 14(1): 26–31.

Srnicek, N., and A. Williams. (2015). *Inventing the Future: Postcapitalism and a World Without Work*. London: Verso.

Tenove, C., H. J. S. Tworek, and F. McKelvey. (2018). *Poisoning Democracy: How Canada Can Address Harmful Speech Online*. Ottawa: Public Policy Forum. Retrieved from <https://

ppforum.ca/publications/poisoning-democracy-what-can-be-done-about-harmful-speech-online/>.

United Nations Convention on the Political Rights of Women. (1952). <http://www.un.org/womenwatch/directory/convention_political_rights_of_women_10741.htm>.

United Nations International Covenant for Civil and Political Rights. (1966). <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

United Nations Universal Declaration of Human Rights. (1948). <http://www.un.org/en/universal-declaration-human-rights/>.

United States Senate Intelligence Committee. (2019a). *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media*. Retrieved from <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf>.

United States Senate Intelligence Committee. (2019b). *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure*. Retrieved from <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf>.

Webster, F. (2014). *Theories of the Information Society*. New York: Routledge.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Address correspondence to:
Holly Ann Garnett
Department of Political Science
Royal Military College of Canada
P.O. Box 17000, Station Forces
Kingston, ON K7K 7B4
Canada

E-mail: holly-ann.garnett@rmc-cmr.ca

Received for publication March 16, 2020; accepted March 25, 2020; published online April 30, 2020.