Joint Statement on Privacy and Democratic Rights

December 8, 2023

Key Takeaways:

- **Privacy is an internationally recognized fundamental right, one that is both an essential precondition for citizens' other freedoms, as well as a keystone right for democracy.**
- **The right to privacy underpins the personal flourishing and development of individuals as citizens, as well as their exercise of social and political freedoms and participation.**
- **Privacy rights and data protection can be viewed as distinct yet overlapping rights, with varied scope and application. However, both specifically and mutually support equality and democratic values.[1]**
- **For example, privacy protection ensures protections for personal beliefs, party associations, safeguards for rights to private communications, living peacefully and free from abuse or infringement, ensuring personal choices in electoral enumeration, free exercise of voting, as well as secret ballots.[2]**

Introduction:

1. **This year, 2023, marks the 75th anniversary of the** *Universal Declaration of Human Rights* **which includes privacy as a fundamental right. As such, the purpose of this joint statement of supervisory authorities from sovereign countries and independent, international organizations is:**
    a. **to provide context and the current landscape around the fundamental right to privacy,**
    b. **draw links with other democratic or independent rights and freedoms,**
    c. **highlight findings from research into privacy as it relates to the democratic process or constitutional principles and commitments[3], and,**
    d. **set out specific expectations for the responsible and ethical management of personal data in these contexts.**

Context and current landscape:

2. ***Global efforts and international law*: International Human Rights Day is an important moment to recount that international legal instruments such as the 1948** *Universal Declaration of Human Rights* **have recognized the fundamental right to privacy, now in place for over seventy years.[4]**
    a. **Member states of the United Nations declared in 1948 that privacy is an inalienable and universal human right.**
    b. **In 1966, the** *International Covenant on Civil and Political Rights* **stressed the central role that privacy plays in democracy.**

3. ***Privacy as a foundation for democracy:* Over the course of the 20th century, privacy rights emerged as a backstop against abuse, oppressive influences, and despotic behaviours.**

a. **Specifically, democratic rights could be curtailed through the exercise of power through the control of and access to detailed information about the identity, thoughts, beliefs, and actions of citizens, or persons contributing to a society or economy.[5]**
b. **Oppressive or anti-democratic actors may do so to influence, nudge, shape, and control the opinions, expression, and behaviours of individuals and this awareness led democratic governments to commit to privacy as a fundamental human right and a pillar to uphold democracy.[6]**

4. ***Privacy as constraint on power*: Treating privacy as a fundamental right means treating it as we do other human rights. Privacy must be legally protected, with a strong, fair, and enforceable rights-based regime.**
    a. **The notion of privacy as an individual's right to control information about themselves emerged in the 20th century, and spread as a legal ideal to be protected, as the rise of authoritarian and totalitarian regimes around the globe catalysed and spread.**
    b. **Given the current pace of technical change, those adopting new technologies need principles and processes to closely assess risks to privacy, equality, fairness, and freedom before using data-driven devices and autonomous or semi-autonomous systems (including artificial intelligence, machine learning, automated decision-making, and profiling).[7]**

Links between privacy and democratic process (observations from research):

5. ***Freedom of personal political belief and expression*: in modern elections, forms of free expression such as online debate, mobilization, and communications have become a critical part in the campaign process.[8] That widening of access and participation can be a democratizing influence.**
    a. **However, given the scale of political messaging and digital strategy in contemporary elections, the scope of the personal information collected by party organizations needs serious regulatory attention and effective regulation under the law.[9]**
    b. **That is because political parties, corporations and a wide range of other actors monitor and track public opinion very closely.[10] Meaningful, enforceable privacy rights protect the free exchange of ideas throughout the political process, up to and including the safeguard of the 'secret ballot', and foster trust in an era of digital surveillance.[11]**

6. ***Freedom of assembly and association:* In many countries, the right to privacy has served as a check upon unfettered governmental power. At their root, privacy rights elaborate a counterbalance both to political scrutiny and ideological pressure.**
    a. **That is because without privacy protections, both philosophical and political autonomy comes under serious risk. Discussing and conferring in confidence, without legal protection for privacy, can be challenging. Data protection laws protect against undue influence and intrusion on forming political opinions, associations, affiliations, or philosophies.[12]**
    b. **However, modern digital platforms and data brokers capture and share much more voter data via networks of organizations and niche firms than ever before. These**

can prove highly susceptible to third-party manipulation, including the interference of hostile foreign states.[13]

7. ***Right to self-determination and autonomy:*** **Policy debates and partisan messaging play out over online platforms now and this change highlights the link between democratic trends and privacy concerns globally.[14]**
    a. **In the past decade, most public political discourse has moved online, frequently into potentially intrusive, relatively unregulated electronic spaces.[15]**
    b. **Communications online and through social media are micro-targeted – often via complex algorithms – and thus different from other forms of interaction.[16]**
    c. **Furthermore, micro-targeting can fragment the political discourse, and that can result in significantly different messaging and commitment for different audiences. Ultimately, that can erode the deliberative nature of democracy, add incoherence to public debate and diminish electoral discourse as well as the notion of a public space for working out solutions collectively.**
    d. **Content delivery is instantaneous, while funding for messaging remains opaque. Consequently, political marketing can be almost impossible to regulate without strong, proactive laws and remedies. Invasive messaging, political polarization, decline in online trust, election interference are all multi-faceted problems that may result without applying such appropriate safeguards and controls.[17]**

8. ***Right to free, fair electoral processes:*** **Attempts to predict the politics and extrapolate the voting intentions of citizens is now widespread. The fundamental privacy right of individuals to access their personal information, request correction and to withdraw consent for its use would curtail these harms to democratic processes.[18]**
    a. **Privacy laws should protect individuals from undue influence and manipulation from organizations.[19]**
    b. **Privacy laws can be part of the legal checks to keep the political process fair, equal, and free of deceptive practices. In other words, part of a framework to protect open, equitable democratic process.[20]**
    c. **Without reasonable assurances of individual autonomy, the political process can be prone to manipulation.[21]**

Specific expectations:

On International Human Rights Day 2023, we the undersigned members of the data protection community agree on the following actions and expectations:

9. ***For Governments and Legislators***:
    a. **Recognition – We call on governments, independent authorities, and independent organizations around the world at all levels to recognize privacy as a fundamental right, essential to the protection of other democratic rights and freedoms.**
    b. **Regulation – We call on these governance bodies to ensure rules for political use of personal information are clearly established, and for their legislative bodies to ensure their jurisdictions' relevant privacy laws are applicable to the collection and processing of personal data undertaken by political parties or similar organizations.**

c. **Review – We reassert the view, in all jurisdictions, that an independent body needs to be empowered to verify and enforce privacy compliance by political parties (or similar influential bodies) through, among other means, investigation of complaints, audits and inquiries.**

10. ***For Political Parties, Influential Bodies, or Partisan Organizations***:
    a. **Strong privacy standards and best practice – We call on political parties and partisan organizations to implement robust privacy policies and strong data protection frameworks. We expect them to respect individuals' privacy and apply international privacy standards.[22]**
    b. **Fair information principles – We expect political parties and partisan organizations to adhere to fair information principles – including strong safeguards, clear information for the public, and provisions for a right of access and correction. This will give meaning to privacy policies and help ensure that personal information is treated in a manner respectful of privacy rights.**

11. ***For Digital Platforms and Data Brokers***:
    a. **Meaningful, informed consent – In the context of their part in the political ecosystem, where consent is the basis for processing personal information tied to political or electoral activity, we expect digital platforms to obtain meaningful, valid consent from users where their personal information is used. That consent must be clear, timely, informed, and explicit.**
    b. **Rigorous data safeguards and policies – We expect digital platforms to put in place and maintain security measures to ensure that personal information in their custody is secure from unauthorized or unlawful access, use or disclosure, particularly where such information relates to the personal data, political beliefs, party involvement or electoral campaigning information of individuals based anywhere in the world.[23]**
    c. **Transparency – We call on digital platforms and online service providers, to the greatest extent possible, to provide regular, public reporting on when and how they respond to government requests for information on users.[24] Organizations should also conduct due diligence and impact assessments or procure written assurance from government or public authorities before responding to such requests.**

12. For Data Protection Offices and Other Regulators:
    a. **Proactive enforcement – As part of our role in protecting electoral process, we call on regulators to actively apply all relevant laws – including privacy, data protection, electoral, and other laws – to the activities of all actors in the socio-political ecosystem.**
    b. **Holistic regulation – Regulators are encouraged to actively pursue cross-regulatory cooperation across electoral, human rights, privacy, and other regulatory spaces as these expectations extend to registered political parties, campaign organizations, commercial data brokers, analytics firms, advertisers, and social media platforms.**

13. ***For Civil Society, Media, and Advocacy Organizations***:

a. Open dialogue and discussion – **Recent history provides examples of despotic practices rooted in state surveillance. Fascism, communism, and generally all forms of oppressive, authoritarian rule have a deep antipathy for privacy in general. Moreover, we have seen how excessive data collection presents a real, demonstrable risk for ideals such as the rule of law and democracy.**
b. Advocacy – **It is crucial to encourage civil society organisations, media networks and citizen groups to vigorously assert the critical importance of privacy rights – through their local laws, policies, or democratic processes – by openly voicing concerns about data misuse, intrusive or disproportionate monitoring, and the use of digital profiling practices or surveillance technologies in general, and specifically in local and national elections.**

Conclusion:

14. **Effective data protection and meaningful privacy rights specifically support democratic ideals, processes, participation, and debate.**
15. **Essential facets of open democracy and fair elections include privacy protections for personal beliefs and party or philosophical association, data safeguards for private communications or, where relevant, political beliefs, and ensuring personal choices for privacy vis-à-vis electoral enumeration, the exercise of franchise, and secret ballots.[25]**
16. **As members of the Data Protection and Rights Protection community globally, we assert the findings and expectations enumerated above, to help ensure that democratic institutions, public discourse, and digital platforms remain strong, open, fair, and accessible for all our citizens.**

Signed by:

- **Philippe Dufresne, Privacy Commissioner of Canada and Chair of the Data Protection and Other Rights and Freedoms Working Group of the Global Privacy Assembly**

- **Ana Brian Nougrères, United Nations Special Rapporteur on the Right to Privacy**

---

[1] **Global Privacy Assembly,** *Privacy and Data Protection As Fundamental Rights: a narrative* **(March 2022), p. 20-22, and Global Privacy Assembly,** *Resolution on Human Rights Defenders* *(October 2016)*
[2] **Global Privacy Assembly,** *Resolution on Privacy as a Fundamental Human Right* **(October 2019).**
[3] **Note that while international organisations members of the Working Group (like the DIFC) may support this Joint Statement and its principles, the discussion in this specific section is more directly related to sovereign states.**
[4] **United Nations, "Human Rights Day: December 10".**
[5] **Global Privacy Assembly,** *Privacy and Data Protection As Fundamental Rights: a narrative* **(March 2022), p. 12-13.**
[6] **Global Privacy Assembly,** *Resolution on the Use of Personal Data for Political Communication* **(September 2005).**
[7] **Ana Brian Nougrères.** *Report of the Special Rapporteur on the right to privacy : Principles of transparency and explainability in the processing of personal data in artificial intelligence* **(August**

2023); see also Global Privacy Assembly, *Resolution on Privacy as a Fundamental Human Right* **(October 2019).**

[8] **United Kingdom. Information Commissioner's Office. "The evolution of political campaigning" from** *Democracy disrupted? Personal information and political influence* **(Jul. 2018).**

[9] **Cathy O'Neill, "The Targeted Citizen" from** *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* **(2016), p. 195.**

[10] **Demos, "The State of the Art" from** *The Future of Political Campaigning* **(July 2018).**

[11] **Colin Bennett and Smith Oduro-Marfo,** *Privacy, Voter Surveillance and Democratic Engagement* **(October 2019).**

[12] **David Flaherty,** *Protecting society in surveillance societies* **(University of North Carolina Press, 1989); Hannah Arendt**, *The Origins of Totalitarianism* **(Harcourt Brace, 1976), p. 139; Alan Westin,** *Privacy and Freedom* **(Atheneum, 1967), p. 25.**

[13] **Colin Bennett and Robin Bayley,** *The Influence Industry: Data Analytics in Canadian Elections* **(June 2018), p. 9-10; see also Parliament of Canada. Standing Senate Committee on Legal and Constitutional Affairs,** *Controlling Foreign influence in Canadian Elections* **(June 2017), p. 2-7.**

[14] **Government of Canada.** *Declaration on Electoral Integrity Online* **(August 2021).**

[15] **Heidi Tworek, "Communications and the integrity of elections" from** *Canadian Global Affairs Institute Policy Perspective* **(September 2018).**

[16] **Tactical Tech**, *Personal Data and Political Persuasion: Inside the Influence Industry and How it Works* **(March 2019).**

[17] **Colin Bennett and Smith Oduro-Marfo,** *Privacy, Voter Surveillance and Democratic Engagement* **(October 2019).**

[18] **Elizabeth Judge and Michael Pal, "Privacy and the Electorate: Big Data and the Personalization of Politics" (October 2014), p. 6.**

[19] **Association francophone des autorités de protection des données personnelles (AFAPDP), Projet de Déclaration de Tunis sur la protection des données personnelles (Octobre 2022), p. 3.**

[20] **Council of Europe, Committee of the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108).** *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* **(November 2021).**

[21] **Daniel Solove,** *Nothing to Hide: the false trade off between privacy and security* **(Yale University Press, 2011), p. 50.**

[22] **For example, the OECD** *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* **(2013), Council of Europe** *Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* **(1981), and, the Global Privacy Assembly** *Resolution on Achieving global data protection standards* **(2023).**

[23] **This includes those individual beliefs which in many jurisdictions are 'identified as requiring additional appropriate safeguards' or 'special categories of data' as noted in Article 6 of the Council of Europe** *Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* **(1981).**

[24] **Global Privacy Assembly,** *Resolution on Transparency Reporting* **(2015)**

[25] **European Union.** *General Data Protection Regulation*. **"Article 9: Processing of special categories of personal data" including (para. 9.1) "political opinions, religious or philosophical beliefs, or trade union membership" (April 2016).**