



Access Now and Digital Rights Ireland Joint Submission to the United Nations Human Rights Council on the Universal Periodic Review 39th Session Third Cycle for Ireland

25 March 2021

About Access Now & Digital Rights Ireland

Access Now is an international organisation that works to defend and extend the digital rights of users at risk around the world. Through representation around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions and convenings such as RightsCon, we fight for human rights in the digital age. As an ECOSOC accredited organisation, Access Now routinely engages with the United Nations (UN) in support of our mission to extend and defend human rights in the digital age.¹

Digital Rights Ireland is an Irish civil liberties group with extensive experience on issues of technology and fundamental rights. Digital Rights Ireland was a plaintiff in the action before the European Court of Justice in *Digital Rights Ireland and Seitlinger and Others* which invalidated the Data Retention Directive, was an *amicus curiae* in *Schrems I*, which found the Safe Harbor decision on data transfers to the United States to be invalid, and was an *amicus curiae* in the US litigation in *Microsoft v. United States*, which prohibited extra-territorial access by the US Government to emails stored in Ireland. In addition to litigation, Digital Rights Ireland regularly participates in advocacy and policy making work at national and European Union level.

I. Introduction

1. The Universal Periodic Review (UPR) is an important UN mechanism aimed at addressing human rights issues across the globe. Access Now and Digital Rights Ireland welcome the opportunity to contribute to Ireland's third review cycle.
2. This submission examines the right to privacy and protection of personal data in Ireland. Specifically, this submission raises concerns regarding Ireland's resolution of cross-border complaints via the EU General Data Protection Regulation (GDPR), and privacy and data protection concerns stemming from Ireland's Public Services Card (PSC).

¹ Access Now, *About Us*, 2021 <https://www.accessnow.org/>

II. Follow up from previous UPR

3. This is the third UPR for Ireland, last reviewed in May 2016 and October 2011 respectively. During the second UPR, Ireland received a total of 274 recommendations, of which 194 were accepted and 80 were noted.² No recommendations explicitly addressed the right to privacy or data protection. The right to privacy therefore remains a severely overlooked right in the Ireland UPR process.
4. Ireland's previous National Report of February 2016 only mentions the right to privacy in the context of marriage and family life.³ Protection of personal data is not mentioned in Ireland's previous National Report. However, the previous Working Group report on the summary of stakeholder submissions highlighted a recommendation from that UPR cycle's joint submission (JS4) by Digital Rights Ireland and Privacy International. JS4 recommended, inter alia, that "the Government ensure that its communication surveillance laws, policies and practices adhere to international human rights law and standards, including the principles of legality, proportionality, and necessity."⁴

III. International, regional & domestic human rights obligations

5. Ireland is a signatory to the Universal Declaration of Human Rights (UDHR) and has ratified the International Covenant on Civil and Political Rights (ICCPR) and both its Optional Protocols.⁵ Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his [*sic*] privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." The UN Human Rights Committee notes that state parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."⁶
6. Ireland is a party to the European Convention on Human Rights (ECHR) which has been incorporated into domestic law with the adoption of the European Convention on Human Rights Act 2003. Therefore, giving effect to Article 8 of the ECHR which affirms the respect for private and family life, home and correspondence. Ireland is bound by the Charter of Fundamental Rights of the European Union, Articles 7 and 8, which relate to the right to privacy and the protection of personal data. Ireland has also ratified the

² UPR Info, *2RP: Responses to Recommendations & Voluntary Pledges: Ireland Second Review Session 25, 2016* https://www.upr-info.org/sites/default/files/document/ireland/session_25_-_may_2016/recommendations_and_pledges_ireland_2016.pdf

³ UN Human Rights Council, Universal Periodic Review - Ireland, *National Report*, 2016, UN Doc A/HRC/WG.6/265/IRL/1 <https://www.ohchr.org/EN/HRBodies/UPR/Pages/IEIndex.aspx>

⁴ UN Human Rights Council Universal Periodic Review - Ireland, *Summary prepared by the Office of the United Nations High Commissioner for Human Rights*, 2016, UN Doc A/HRC/WG.6/25/IRL/3, <https://www.ohchr.org/EN/HRBodies/UPR/Pages/IEIndex.aspx>

⁵ OHCHR, *Status of Ratification Interactive Dashboard*, 2021 <https://indicators.ohchr.org/>.

⁶ UN Human Rights Committee, CCPR General Comment No. 16, 1988, at para 1.

Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.⁷

7. Irish law provides a statutory right to data protection which is primarily provided for in the Data Protection Act 2018, implementing the EU Data General Data Protection Regulation (EU) 679/2016.
8. The ePrivacy Regulation 2011 protects the right to privacy and confidentiality of communications for phone, e-mail and Internet use, and gives effect to the EU ePrivacy Directive 2002/58/EC.⁸
9. The Constitution of Ireland does not explicitly guarantee a right to privacy, but the courts have recognised an unenumerated right to privacy as one of the personal rights in the Constitution.⁹

IV. The right to privacy and data protection in Ireland

General Data Protection Regulation and Ireland's role within the One Stop Shop

10. The EU General Data Protection Regulation (GDPR) entered into application in 2018. In May 2019 and 2020, Access Now published reports examining the implementation of the law, highlighting the particular role that the Irish Data Protection Commission (DPC) has to play in the resolution of cross-border complaints.¹⁰ The reports examine national implementation and internal challenges, such as the limitations of the mechanisms established for enforcement of the GDPR, particularly the lack of cooperation among data protection authorities (DPAs) and the lack of resources to do their work.¹¹
11. The GDPR establishes a mechanism for cooperation and consistency in the application of the law to cross-border investigations. This system is based on the “one-stop-shop” mechanism which is supposed to serve both people and companies. Through this system, users can bring a data protection complaint to the authority in the country where they live, even if the company against which they lodge the complaint is established in another EU country. Meanwhile, companies can designate a lead authority which will be tasked with handling all complaints about them, regardless of where the complaint has been filed. The lead authority has to cooperate with other authorities where people may file complaints. Nearly three years after the GDPR became applicable, and despite the fact that many cross-border cases have been submitted to authorities, the system has yet to be fully tested for the resolution of cross-border cases.

⁷ ETS No. 108.

⁸ As amended by Directive 2006/24/EC and 2009/136/EC.

⁹ *McGee v Attorney General* [1974] IR 284; *Kennedy and Arnold v Attorney General* [1987] IR 587.

¹⁰ Access Now, *One Year Under the GDPR: An Implementation Progress Report*, 2019, <https://www.accessnow.org/cms/assets/uploads/2019/06/One-Year-Under-GDPR.pdf>.

¹¹ Access Now, *Two Years Under the EU's GDPR: An Implementation Progress Report*, 2020, <https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf>.

12. A large number of global tech companies have chosen Ireland as their main establishment under the GDPR. This means that Ireland and the DPC have a central role in the application of the GDPR and that the Irish authority is responsible for handling a large number of cases. However the disproportionate weight put on a single authority for the application of the GDPR threatens to undermine the effectiveness of the one-stop-shop system.¹²
13. The most visible issue is delay. At the time of writing, the DPC has reached a final decision in only four of 196 cases in which it is the lead supervisory authority.¹³ This has prompted criticism from the European Parliament and other national supervisory authorities.¹⁴
14. As already highlighted in the Access Now implementation reports on the GDPR, there are several overlapping reasons for these delays but in the Irish context the main element appears to be ongoing underfunding of the DPC.¹⁵ The DPC has described itself in its most recent pre-budget submissions as being “acutely strained” when facing the “disproportionate resources” of tech firms and as lacking a “fit-for-purpose management and organisation structure” due to the failure to receive increased funding to facilitate its new role as de facto regulator of the internet industry across Europe.¹⁶

A digital card as a condition to receive public services: Ireland’s Public Services Card (PSC)

15. Digital identity systems form the basis of many welfare activities in various jurisdictions. Infrastructural lapses lead to severe on-ground adversities in the lives of the beneficiaries. It is imperative that digital identity systems, particularly those foundational systems backed by the state’s resources and legal powers, are designed around sound principles of governance, data protection, privacy security and non-discrimination.¹⁷
16. Governments, such as Ireland, are increasingly relying on digital technologies to make the delivery of services, including welfare benefits, more efficient and accurate, and to reduce corruption by using technologies to assist in clear identification and secure

¹² McIntyre, ‘Regulating the Information Society: Data Protection and Ireland’s Internet Industry’, in *Oxford Handbook of Irish Politics*, ed. David Farrell and Niamh Hardiman (Oxford: Oxford University Press, 2021), <https://ssrn.com/abstract=3520101>.

¹³ The Irish Times, *Irish data regulator sparks row with EU colleagues on Facebook oversight*, 2021, <https://www.irishtimes.com/business/economy/irish-data-regulator-sparks-row-with-eu-colleagues-on-facebook-oversight-1.4513065>.

¹⁴ McIntyre, ‘Regulating the Information Society: Data Protection and Ireland’s Internet Industry’, in *Oxford Handbook of Irish Politics*, ed. David Farrell and Niamh Hardiman (Oxford: Oxford University Press, 2021), <https://ssrn.com/abstract=3520101>.

¹⁵ Id.

¹⁶ The Irish Times, *Data Protection Commission ‘acutely strained’ by big tech cases*, 2021, <https://www.irishtimes.com/business/technology/data-protection-commission-acutely-strained-by-big-tech-cases-1.4457683>

¹⁷ Access Now, *National Digital Identity Programmes: What’s Next?* 2018, <https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf>.

authentication. However, these programmes can themselves become impediments to governance, harm the provision of welfare services, further marginalize individuals, and put users' privacy rights at risk. Without proper human rights safeguards that are rigorously followed, digital identity systems can be counterproductive to the welfare of the people, violate internationally protected human rights, and undermine cybersecurity.

PSC's disproportionate impact on the privacy rights of those living in poverty, including persons with disabilities, and other marginalized groups

17. Although Ireland's Public Services Card (PSC) is not an identity card, it seeks to collect and collate individual's personal data as a condition for receiving government services, including access to social welfare benefits. Those accessing such social welfare services already face intersecting barriers and marginalization. As such, their privacy rights are more at risk through their reliance on Ireland's PSC.¹⁸
18. On 21 April 2020, the former UN Special Rapporteur on extreme poverty and human rights, Philip Alston, warned that Ireland's PSC "discriminates against the marginalised" as it is "being implemented in ways that gravely prejudice the least well-off."¹⁹ According to Alston, "too many of those living in poverty, including people with disabilities and other marginalised groups, are unable to get the support they need as a result of the requirements involved in obtaining the PSC."²⁰ Therefore, as captured by the Special Rapporteur, unlike the well-off, "those who rely on the government for assistance have no choice but to give up their privacy and dignity in order to get help."²¹

Grave concern over the collection of biometric data shared amongst government databases

19. We note grave concern over Ireland's use and collection of biometric data in the PSC, which continues to be shared amongst government databases.²² The collection and use

¹⁸ See Elizabeth Farries, *Bartering your privacy for essential services: Ireland's Public Services Card*, Digital Freedom Fund, 2019, <https://digitalfreedomfund.org/bartering-your-privacy-for-essential-services-irelands-public-services-card/>

¹⁹ OHCHR, *Ireland's Public Services Card discriminates against the marginalised, warns UN rights expert*, 2020, <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25811&LangID=E> The Special Rapporteur's statement follows the publication of an official communication sent to the Irish Government on 14 April 2020, "expressing his concerns about the PSC and asking detailed information about its implications" for more information See Mandate of the Special Rapporteur on extreme poverty and human rights, Reference OL IRL 1/2020, <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25176>

²⁰ OHCHR, *Ireland's Public Services Card discriminates against the marginalised, warns UN rights expert*, 2020, <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25811&LangID=E>

²¹ Id.

²² Id.

of biometric identifiers — including fingerprints, iris scans, and facial geometry, among others — pose significant risks for individuals. While biometric data is vulnerable to hacking, just like other authentication methods, unlike a password, biometric indicators cannot simply be reset or changed as needed.²³ This poses a higher security risk, since it becomes increasingly difficult to repair the damage done by leaks or hacks of biometric data, and therefore restore sanctity to biometric-based systems.

20. Given the potential for exploitation of this data, we discourage the use of biometrics in any form of a digital identity program or system. The aggregation and use of biometric data should be sharply limited, even if such aggregation and use is aimed at increasing convenience or justified as a way to enhance security.

Ireland's PSC deemed illegal by Ireland's Data Protection Commission, but the government persists with its use

21. In August 2019, the DPC found that individual's privacy rights were violated by the extension of the PSC beyond core social welfare benefits, including unlawful sharing of individuals' data.²⁴ Based on the finding, the Data Protection Commission found that the Government must cease the practice of requiring a PSC as a precondition for access to wider public services. However, the Government continues to refuse to comply, instead bringing an unprecedented set of legal challenges to the findings of the regulator.²⁵
22. Multiple public bodies in Ireland have illegally refused services to citizens without a PSC. Such instances include: passport applications denied by the Passport Office, driving license renewals refused by the National Driver Licence Service, parents refused a school bus appeal by the Department of Education and Skills, pensions cut off by the Department of Employment Affairs and Social Protection.²⁶
23. Overall, the PSC has unlawfully spread across departments, functionally turning the PSC into a national identity card without legislation or debate.²⁷ Despite being told that this extension of the PSC is illegal the government of Ireland continues to: process personal and biometric data, hold personal PSC data "indefinitely", illegally withhold vital services from citizens without PSCs across multiple departments even amid the pandemic, and illegally share PSC data from the Department of Social Protection to other entities.

V. Recommendations

24. Data protection and the right to privacy should be prominent issues in Ireland's upcoming UPR review cycle. We therefore recommend that the Government of Ireland:

²³ Access Now, #WhyID, 2019, <https://www.accessnow.org/whyid/>

²⁴ Data Protection Commission, *DPC Statement on Matters Pertaining to the Public Services Card*, 2019, <https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-matters-pertaining-public-services-card>.

²⁵ Digital Rights Ireland, #no2psc, <https://no2psc.digitalrights.ie/>.

²⁶ Id.

²⁷ Id.

- a. Refrain from infringing the right to privacy of those living in poverty, including persons with disabilities, and the rights of other marginalized groups, by requiring individuals to provide their personal data and information to the PSC in order to access social welfare services.
- b. Develop legal procedures and evidentiary standards for the collection of biometric data with care to protect human rights and due process. Refrain from collection and use of biometric data until it can be proven that such biometric authentication is completely safe, inclusive, not liable to error, and is the only method of authentication available.
- c. Formally recognize and comply with the August 2019 findings of Ireland's Data Protection Commission that the operation of the PSC is illegal. Specifically, Ireland should stop all of the following until further notice:
 - d. Requiring biometric data through the PSC;
 - e. Withholding vital services, particularly amid the COVID-19 pandemic, from citizens without PSCs across multiple departments;
 - f. Sharing PSC data with other departments by the Department of Social Protection; and
 - g. Holding personal PSC data indefinitely.
- h. Provide adequate funding for the Irish Data Protection Commission and carry out a review to identify legal changes necessary for it to carry out its functions more expeditiously.

25. The UPR is an important UN process aimed at addressing human rights issues worldwide. It is a rare mechanism through which citizens around the world get to work with the government to improve human rights and hold them accountable to international law. Access Now and Digital Rights Ireland are grateful for the opportunity to make this submission.

For more information, please contact: un@accessnow.org & contact@digitalrights.ie