Aston University
BIRMINGHAM UK

IALS INSTITUTE OF ADVANCED LEGAL STUDIES | SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON

Policy Report

‘Making “Digital Streets” Safe? Progress on the Online Safety Bill’
June, 2023

Edited by Dr Edina Harbinja and Dr Nora Ni Loideain

1. Introduction

At the time of writing this report, the House of Lords is debating the Online Safety Bill. This potentially landmark law would establish a regulatory framework for certain online services. These include major international companies which provide user-to-user services, such as Facebook (Meta), and search services, such as Google (Alphabet).

The UK Government's dual aims in introducing the Online Safety Bill are 'to make Britain the best place in the world to set up and run a digital business while simultaneously ensuring that Britain is the safest place in the world to be online.'

On 27 and 28 March 2023, the Information Law & Policy Centre (ILPC) (Institute of Advanced Legal Studies, University of London) and its Director, Dr Nora Ni Loideain, co-hosted with Dr Edina Harbinja (Aston University) an international and multi-disciplinary conference. This event brought together experts from across academia, policymaking, and civil society to critically examine and discuss recent developments concerning the proposed Online Safety Bill. Panels addressed the development and future of these developments for regulation, policymaking, and governance within the UK and internationally.

The roundtable on Day 2 was co-hosted by Lord Colville of Culross. Lord Colville first got involved with the Bill in 2017 as a member of the Lords Communications and Digital Committee. He has put forward a number of amendments, including the amendment to reduce Secretary of State's powers to direct Ofcom and amendments aimed at protecting free speech.

2. Overview of Online Safety Bill

In April 2019, the UK Government's Department of Digital, Culture, Media and Sport (DCMS) released its White Paper on 'Online Harms'. This promised to establish in law a duty of care towards users by platforms overseen by an independent regulator.[1] The crux of the White Paper included a proposal for a new regulator. This body would be empowered to decide what activities and content are deemed harmful to Internet users.[2] After making this decision, it was envisaged that the regulator could mandate intervention by Internet providers to protect users from harms.[3]

Departing from a major proposal set out in the White Paper, the Draft Online Safety Bill (published in May 2021) dropped a controversial suggestion put forward by the Carnegie UK Trust to establish an overarching duty of care for platforms (service providers). Instead, the Draft Online Safety Bill introduced several specific duties of care.

In another significant change to the White Paper, the UK Government decided against the idea of establishing a new regulator. Instead, it is proposed that Ofcom (an existing regulator for communications) will be tasked with significant powers to implement and enforce the Online Safety Bill.

After a difficult period of political turmoil, consultations, and delay, the Bill was introduced to the Parliament in March 2022. The Bill confined harm to 'physical or psychological harm' and set out in detail a series of discrete duties, some based on harm and some on the illegality of various kinds. These include the illegality safety duty for U2U services, the illegality safety duty for search engines, the 'content harmful to adults' safety duty for Category 1 (large high-risk) U2U services and the 'content harmful to children' safety duty for U2U services likely to be accessed by children.

[1] Online Harms White Paper: <www.gov.uk/government/consultations/online-harms-white-paper> (last updated 12 February 2020).

[2] Online Harms White Paper (CP 57, April 2019) paras 2.2 and 5.15: <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf>.

[3] Ibid, para 6.5.

The Online Safety Bill was considered by a Public Bill Committee between May and June 2022, with a line-by-line examination of the Bill. In this phase, the Government added new provisions (such as Schedule 2). Clause 129 was also amended so that Ofcom would have to consult the Information Commissioner's Office (the UK's data protection regulator) before publishing guidance on using its enforcement powers.

On 12 July 2022, the first day of the report stage took place. Government amendments were added at this time to the Bill relating to journalistic content, adult safety duties, and illegal content duties. The second day of the report stage occurred on 5 December 2022 and new Government clauses and amendments were agreed upon.

The Government announced plans to amend the Bill on 28 November 2022. This included removal of the controversial 'legal but harmful' provisions for adults to protect freedom of expression. In addition, the Government introduced new clauses and amendments were made after two committee sittings in December 2022. The adult safety duties were removed, and new user empowerment tools for adults were introduced.

3. Online Safety Bill: Important developments in 2023

In January 2023, the Government announced that it would be amending the Bill in the House of Lords to strengthen the provisions on senior management liability and combat illegal small boat crossings. Following the third day of the report stage, and the third reading on 17 January 2023, the Bill was introduced in the House of Lords on 18 January 2023.

The Bill is currently at the Committee Stage in the House of Lords. The debates and proposed amendments sparked some optimism that the scrutiny could address critical concerns around free speech, illegal content, privacy, encryption, regulatory independence and oversight in particular.

The most significant amendments align with what was discussed and concluded in our workshop held at IALS and the House of Lords in March 2023.

3.1. Scope of the Online Safety Bill

Speakers agreed that the Bill has a very wide scope, and that the legislation is intended to address many challenges. In many instances, these involve competing areas of public interest and incompatible issues: child protection; free speech; communication offences; illegal content; immigration; discrete offences such as cyber-flashing etc.).

Several participants spoke in favour of the Bill on the main ground that it was important it went forward in some form. However, most participants expressed concerns that the proposed regime in its current state is cumbersome and inconsistent. One commentator referred to the Bill as being akin to 'a Christmas tree' overburdened with multiple aims. In particular, the original primary aim of protecting children online has been expanded to include compatible and conflicting aims. The latter of which threaten to undermine safety, encryption, and digital rights on the Internet.

Baroness Stowell, for instance, expressed her concern about the wide scope of the Bill and would have preferred if the primary focus had remained as child safety online. She notes that a significant challenge is improving the Bill without it becoming even more complex and having further unintended consequences. At the same time, she emphasised the need to be realistic in terms of what can be achieved at this stage of the drafting process. She gave a good overview of some of the issues that the House of Lords is reviewing, ranging from Clause 39 and powers that will be allocated to Ofcom to the removal of legal but harmful provisions and how the alternative to that measures up in terms of implications on freedom of expression.

She raised an important point that the Online Safety Bill is not the only relevant proposed legislation in this space. It should not therefore be considered in isolation from other pieces of related legislation, such as the Digital Markets, Competition and Consumer Bill.

Dr Nora Ni Loideain (IALS, University of London) reiterated the significance of not scrutinising the Online Safety Bill in a legal and policymaking vacuum. She highlighted that the Data Protection Act 2018 and the Human Rights Act 1998 (HRA) are also relevant to many of the safeguards and human rights that will be affected by the Online Safety Bill. These include (but are not limited to) the right to private life, the right to freedom of expression, and the right to non-discrimination. The Bill should also explicitly reference its compliance with the HRA and protected rights therein.

Professor Lorna Woods OBE (University of Essex) also raised an issue of giving powers to the Secretary of State and the clarity between the legislation and its wider framework of statutory instruments. She especially stressed the fact that the Online Safety Bill will be a significantly complicated piece of legislation once it is enacted. Professor Woods explained that the Bill was a 'framework' bill, the bones of which would need to be fleshed out by secondary legislation and codes of practice.

In terms of the Bill's remit, Professor Woods highlighted that there are two main categories of content – criminal and content harmful to children. Both of these have general definitions in the Bill. However, it is possible that difficulties may arise with identifying priority content that is going to be subject to more detailed rules. There is priority criminal content in Schedules 5, 6, and 7, such as terrorism, Child Sexual Abuse and Exploitation (CSAE), and a random selection of criminal offences.

But there is a gap in the regulation of content harmful to children, and this makes it difficult to assess the regime – is it focusing on the right things? Further, what is the difference between priority and primary priority content? She also raised the question of who is making the choices. The Bill now requires Ofcom to report on instances of harm that are listed as priority content, but this does not constrain what the government does. It is merely advisory.

On further issues related to the scope of the Online Safety Bill, Professor Woods also highlighted the power of the Secretary of State to change exemptions and the lack of reasoning behind subjecting Categories A, 1 and 2A to a higher regulatory regime. These issues, she stressed, have not been given the close scrutiny and attention that they deserve.

On Day 2, Maeve Walsh expressed the desire for the Bill to require greater accountability and transparency from tech platforms and called for the duties to be made more robust.

Mark Johnson (Big Brother Watch) shared this key concern about the broad scope of the Bill. Adding that the Bill does not mention anything about the 'surveillance capitalism' systems that have become prominent. In his view, the 'big players do not resist this legislation because it only strengthens their products and services – the more they have to moderate, the more data they can collect for their services'. Consequently, he argued that the Bill may serve to further exacerbate the challenges in regulating platforms 'rather than curtail their powers'.

3.2. Oversight and implementation

All contributors agree that implementing the Online Safety Bill on time and in a manner that maintains public confidence would be a significant challenge. Some argued that it would also be problematic to have no Bill.

Regarding oversight and balance of powers, Baroness Stowell believes that the long-term success of the Bill's implementation will rely on having a good oversight mechanism in place. There must be agreement on the overarching regulatory framework, and there must be clarity about who holds power over what. In her opinion, the key priority of the House of Lords should be to get the 'fundamentals' of the framework right and have appropriate checks and balances in place. In her view, the key thing is getting the balance of power right between Parliament, the Government, Ofcom, and the tech platforms. She expressed her concerns that the independence of Ofcom could be undermined, potentially damaging its ability to hold tech platforms to account.

The first policy change that the Committee she chairs has proposed is to reign in some of the Secretary of State powers in Clause 39 of the Bill. Clause 39 allows the Secretary of State to direct Ofcom to change its codes of practice on regulating social media platforms for reasons of public policy. This, in her opinion, is an unnecessary interference. The Government has suggested clarifying this clause with a list of purposes, such as security, foreign policy, economic policy, and burden to business. But the list is quite expansive, vague and uncertain in scope, to the extent that almost anything could be included. Hence, the interference is not justified from a rule of law perspective or on grounds of proportionality.

The Committee proposes changing Clause 39 to allow the Secretary of State to write to Ofcom with observations on national security and child safety, and if the information is sensitive, then public letters can be supported with private correspondence. Clause 39 also allows the Secretary of State to direct Ofcom into a private form of ping-pong as it develops codes of practice, and this could go on indefinitely with no parliamentary oversight hence she proposes changing the clause so that the Secretary of State does not have the power to delay Ofcom codes indefinitely. While public safety and national security are important, Baroness Stowell emphasised that an appropriate balance must be ensured.

Additionally, while the Secretary of State should not have excessive powers, it is necessary to ensure that Ofcom as the regulator, is scrutinised and held to account as it would have enormous influence and powers. Baroness Stowell proposes setting up a Joint Committee of Parliament to scrutinise digital regulation across the board and to ensure parliamentary oversight of Ofcom. She believes this would address many concerns raised about implementation and keeping pace with digital developments.

Professor Woods raised concerns about the powers of the Secretary of State to change exemptions, noting that the Secretary of State has very similar powers for changing exemptions in the Data Protection Bill. Like Baroness Stowell, she also raised concerns about the power of the Secretary of State to direct codes of practice, the exceptional circumstances provision, and Clause 157 (guidance on the implementation of powers). These clauses, she believes, interfere with the day-to-day running of the regime.

Although Clause 157 is only guidance, Professor Woods finds the scope of the clause very wide-ranging and the lack of justification for such a wide scope is problematic. The power given to the Secretary of State to direct codes of practice is deeply problematic because the government lacks knowledge about technical detail. Codes of Practice are about the implementation of the regime. They are about the features, characteristics, design, and operation of the service and not about identifying particular items of content to take down. She, therefore, questions what that power to interfere actually does to the way the regime could work.

Dr Martin Husovec (London School of Economics and Political Science) also highlighted a major problem of enforcement, namely that the Online Safety Bill focuses solely on service providers. In contrast, the EU Digital Services Act has a system where there can be an ex post review of decisions by external bodies, which again incentivises providers to make precise decisions. This, again, is a missed opportunity for the Bill. He raises two key questions regarding the scope of the Bill. Why not broaden the focus and engage institutions more broadly in society? Secondly, why not focus on the entire ecosystem?

3.3. The Illegality Duty

A significant issue identified by the contributors, particularly Graham Smith (Bird and Bird) and Dr Edina Harbinja (Aston University), is the illegality duty. The Online Safety Bill imposes positive obligations on both digital services/social media platforms and search engines in relation to illegal content.

Graham Smith spoke about this duty in detail. In summary, illegal content must be taken down once detected, according to clause 170. The Bill also introduces new criminal offences, such as false communication offences. Smith highlighted some of the problematic assumptions being made about the Bill regarding illegal content. In particular, the mantra that 'what is illegal offline is illegal online' does not recognise that the Bill embodies a different kind of legal regime from that which applies to individual speech offline. Secondly, the Bill is 'not focused only on regulating Big Tech – its core duties and principles (systems and processes) apply to all kinds and sizes of user-to-user platform.'

One of the key issues with Clause 170, Smith argues, is that the platforms will be required to remove too much of the user content, thus curtailing free speech. The platforms are required to find illegality if they have 'reasonable grounds to infer' that the elements of the offence are present, including factual elements and mental elements. In this context, the most important issues are likely to be intent and whether the user has an available defence (such as a reasonable excuse). Under the Online Safety Bill, unless the platform has information on the basis of which it can infer that a defence may successfully be relied on, the possibility of a defence is to be left out of consideration.

The Bill requires platforms to determine illegality on the basis of information reasonably available to them. This raises concerns about the context in which the information is shared and available and the paucity of information in the case of proactive, automated real-time filtering. Such a system can work only on user content that it has processed, which would omit extrinsic contextual information.

According to Smith, as a result, the Bill's approach would lead to compulsory filtering and removal of legal online content at scale, not comparable to offline removal. The illegality duty is a form of prior restraint since the Bill requires content filtering and removal decisions to be made before any fully informed, fully argued decision on the merits takes place. Dr Harbinja agreed with this and emphasised the need to introduce the 'manifest illegality' standard instead of the 'reasonable grounds to infer', as she also proposed on various occasions to committees during the Bill's.

On Day 2, Dr Monica Horten (Open Rights Group) spoke about Clause 9 and how this provision could also be seen as imposing prior restraint on free speech, emphasising that content could be removed by intercepting the content whilst the user was uploading it, and before it could appear on the platform. This is potentially what is meant by the requirement for online platforms to 'prevent users encountering' illegal content. Such removals would be carried out at scale. It is sometimes known as an upload filter. Users would not know why their content did not appear, and in the event of false flags, this would be a restriction on lawful content.

Beatriz Kira (Department of Political Science, UCL) noted a wider content-related issue on Day 2. She focused on user empowerment tolls currently envisaged in the Bill, noting that the Bill does not encourage enough other content management. In her view, user improvement tools need to be made more effective.

3.4. Free Speech

Most of the participants agree that the Online Safety Bill represents a threat to free speech, which will encourage online services to be excessively zealous in removing perfectly legal content from their platforms in order to avoid fines. Mr Feeney noted that there is a categorisation issue – the worthiness or unworthiness of content depends on context. In this view, the Bill's design reveals a misunderstanding of how content moderation at scale works, neglecting the fact that, in many cases, the harm associated with the content is caused by the context in which the content was shared rather than the content itself. The context must be taken into account; content of historic, artistic, educational, and documentary significance could be automatically removed, and this would have a chilling effect on free speech.

Professor Paul Bernal (University of East Anglia) noted that the idea that the Bill protects freedom of expression is wrong. The Bill is a massive intrusion into privacy, and partly through it, it chills freedom of expression. He noted that the Bill is premised on the belief that 'we want safety, and the way to do that is to chill harmful speech'. He explained the various levels of the chill: intentional chill, which comes from legislation, chills from companies reacting to the Bill, and lastly, the chills from how people behave in response to the legislation. The third chill depends on what people think is in the legislation or on what they are told by the politicians and media.

Consequently, people may be removing themselves from online platforms, reducing the amount of potentially good material available to access. Additionally, the prospect of the Bill being used as a tool of authoritarianism to shut down political dissent and opposition is a danger. Mr Johnson also expressed related concerns that the Bill rips up existing domestic and international freedom of expression standards and how it could be used as a tool of authoritarianism. Privacy concerns are intrinsically related to free speech concerns. For example, Professor Bernal warned of the use of real names and age verification as another chill on freedom of expression. If real names are forced, people on the margins will be restricted from expressing their views.

Dr Harbinja noted the vague distinction between democratic and journalist content, as set out in clauses 15 and 17 of the Bill. This has been exacerbated by the inclusion of clause 16 and the news publisher content. The three clauses aim to protect equally essential aspects of speech but offer very different protection mechanisms and remedies (e.g., 'a dedicated and expedited complaints procedure' for journalistic content in clause 17 or a detailed explanation of steps to be taken regarding the news publisher content in clause 16). Further, the content of democratic importance seems to include only political speech, which is much more restricted than categories of speech protected by Article 10 ECHR. She also mentioned clause 20 (Duties about freedom of expression and privacy), noting that she had submitted specific amendment proposals to the Parliament, which would clarify and strengthen this clause. The clause, as drafted, conflates concepts of privacy and data protection and does not signal a clear intent to protect freedom of expression, privacy and users' personal data. Therefore, she proposed that in clause 20, words 'have regard to the importance of protecting' are replaced with the word 'protect'.

On Day 2, Professor Sonia Livingstone (LSE) spoke about the effects of the Bill on children and their free speech. In her view, from a children's rights perspective, the Bill could be valuable if it protects children from online risks yet problematic if it results in locking children out of services that they use and could be valuable for their development.

3.5. Privacy and encryption

Most participants criticised the current phrasing of Clause 110 and its possible adverse effects. This provision allows Ofcom to, after issuing a warning, give notice to user-to-user services or search services to use accredited technologies to identify and take down swiftly child sexual abuse content, whether it is communicated publicly or privately. Services might also be obliged to develop systems equivalent to such accredited technology to identify child sexual abuse content.

The term 'privately' is problematic because it leads to the inclusion of private messengers into Clause 110, which is excluded from the other parts of the Bill. Private messenger services are end-to-end encrypted, and this clause calls for scanning encrypted messages for child sexual abuse content. Scanning requires clear text. It can be implemented on private messaging platforms by introducing back-doors into the system on the server, or by intercepting messages on the users' device, before they are encrypted for transmission (known as Client-Side Scanning). Clause 110 does not mandate any particular technology, but it is understood that client-side scanning is the government's preference.

Matthew Feeney (Centre for Policy Studies) noted that the Bill could impose obligations on online services that would weaken or remove encrypted communication services and encourage them to engage in greater surveillance of their platforms. The Bill allows Ofcom to mandate the weakening of end-to-end encryption provided by WhatsApp and Signal. Mr Feeney and Dr Harbinja had already proposed an amendment to address these concerns. Professor Bernal warned that the problem with this clause is that accredited technology does not exist in the way that it is hoped to. When a technology is 'accredited' – Ofcom is effectively saying that this particular technology meets certain standards of accuracy in identifying and taking down child sexual abuse content.

Dr Michael Veale (UCL) also highlighted the problems associated with monitoring technology. Whether it is being biased, producing false positives etc. He explained that the use of Client-Side Scanning is a techno-solutionist approach. Dr Veale then stressed how easy it could also be to circumvent and bypass these technologies and how people could be trained to do so. He argued that, given that the upsides of Client-Side Scanning are fairly limited, it is quite dangerous firstly because it is a way for corporate and state surveillance to piggyback onto encrypted messages. These concerns are consistent with those raised by other leading computer science experts who have argued that the only effective way to detect online grooming of children and other forms of CSAE is user reporting.[5]

Dr Veale concluded by explaining that global governance of such scanning technologies would be extremely tricky. The UK is opening Pandora's box, and other countries are also working on their legal standards and rules for scanning technologies. There is no discussion in the Bill of creating an international community that has discussions around this at an international platform. On Day 2, Dr Monica Horten also spoke about the scanning of encrypted messages and its unintended consequences, i.e. the mass surveillance of more than 40 million people in the UK who use encrypted messaging.

In terms of the Government's position on the necessity for the Online Safety Bill, Professor Bernal pointed out that the campaign 'no place to hide' is fundamentally problematic as we all need to hide, and we need the ability to make ourselves safe. The Bill, he argues, does exactly the opposite and has the ability to make large numbers of people less safe unless something is done directly to protect encryption and anonymity.

[5] See Ross Anderson and Sam Gilbert, Online Safety Bill: Policy Brief (Bennett Institute for Public Policy 2022) para 5.2: <https://www.bennettinstitute.cam.ac.uk/publications/online-safety-bill/>.

3.6. Competition

The final major criticism of the Online Safety Bill that arose from the concerns discussed at the workshop is that it will hamper competition and innovation. This is because of the range of costs associated with compliance with Bill's obligations, which are expected to be extremely significant. This provides incentives to smaller firms to sell to Big Tech companies. This is worrying for firms on the edge, such as Wikipedia.

In addition to these anti-competitive implications, geo-blocking was discussed as an alternative to companies completely pulling out of the UK. Companies would provide a different, modified service in the UK, which again is a restriction on freedom of speech with broader implications for consumer rights. Relatedly, the effects of the Bill as a problematic precedent for other countries (particularly those with questionable records of respecting human rights and the rule of law) and the challenges facing its exterritorial application in practice were also discussed.

4. Conclusion and Policy Recommendations

Many participants shared the view that the Online Safety Bill as a whole should be abandoned. However, there was an acknowledgement that this may not be realistic at this point in time. As one commentator observed, a main fallacy in relation to the Bill is 'the sunk cost fallacy, namely we have spent so much time on the Bill, we might as well pass it now'. This Report, therefore, includes the following specific and realistic recommendations as to how the Bill could be improved in the House of Lords. Contributors discussed achievable changes and on the basis of these discussions the authors of this paper (reflecting the views of the majority, but not all discussants) propose the following:

Clause 110 – take out the word 'privacy' to address the concerns about encryption and privacy;

Clause 170 – replace the test of 'reasonable grounds to infer' with 'manifest illegality';

Clauses 39 and 157 – limit Secretary of State powers to direct Ofcom. Ofcom's independence and capacity should also be strengthened with additional resources.

The speakers had an opportunity to review the draft report and the final version will be circulated to MPs, Lords, the Government, the media, and other interested parties.

Acknowledgements

Ms Shrutika Gandhi (IALS, University of London) and Ms Tenishia Prah (University of Aston) for note-taking and general event assistance.

Our thanks to all the contributors and the audience on Day 1 of the workshop and to Lord Colville for hosting us on Day 2.

Contributors

Day 1

Chair: Dr Nóra Ní Loideain, Director and Senior Lecturer in Law, Information Law & Policy Centre Institute of Advanced Legal Studies, University of London

Speakers

Panel 1

Baroness Stowell of Beeston MBE, Member of the House of Lords

Prof Lorna Woods, Professor of Internet Law, University of Essex

Graham Smith, Of Counsel, Bird & Bird

Matthew Feeney (discussant), Head of Technology & Innovation, Centre for Policy Studies

Panel 2

Prof Paul Bernal, Professor of IT Law, University of East Anglia

Dr Michael Veale, Associate Professor, Faculty of Laws, UCL

Dr Martin Husovec, Assistant Professor of Law, LSE Law School

Dr Edina Harbinja, Reader in Law School of Law, Aston University

Mark Johnson (discussant), Big Brother Watch

Day 2

Round Table discussion at the House of Lords with Lord Colville of Culross

Speakers:

Prof Paul Bernal

Matthew Feeney

Dr Edina Harbinja

Dr Monica Horten, Policy Manager – Freedom of Expression at the Open Rights Group

Dr Martin Husovec

Mark Johnson

Dr Beatriz Kira, Research Fellow in Law & Regulation, UCL

Prof Sonia Livingstone, Professor of Social Psychology, LSE

William Moy, Chief Executive. Full Fact

Dr Nora Ni Loideain

Graham Smith

Dr Michael Veale

Maeve Walsh, Associate with Carnegie UK Trust

Report editors

Dr Edina Harbinja is a Reader in Media/Privacy Law at Aston Law School, Aston University. Her principal areas of research and teaching are related to the legal issues surrounding the Internet and emerging technologies. Edina is a pioneer and a recognised expert in post-mortem privacy, i.e., privacy of the deceased individuals. She has published widely on aspects of technology law and regulation, including online safety. Edina holds LLB from the University of Sarajevo, Bosnia and Herzegovina, and LLM (IT and Telecommunications) degree from Strathclyde University, Glasgow. She was awarded a PhD in law from Strathclyde University.

Edina holds a number of appointments and memberships outside Aston. This includes, inter alia, membership of the Advisory Council at Open Rights Group, Senior Fellowship of the Higher Education Academy, membership of the Executive Committee, British and Irish Law, Education and Technology Association (BILETA). Edina is a chief editor for the EUP book series 'Future law' and a deputy editor of the Computer Law and Security Review (CLSR).

She has been a visiting scholar and an invited speaker to universities and conferences in the USA, Latin America, Asia and Europe. She has been able to influence and inform American, the UK and Australian legislators and court cases over the past fifteen years, as well as big tech companies, the legal profession and civil society.

Find her on Twitter at **@EdinaRl**.

Dr Nora Ni Loideain is Senior Lecturer in Law and Director of the Information Law & Policy Centre at the University of London's Institute of Advanced Legal Studies. Her research focuses on EU law, European human rights law, and emerging technologies, particularly within the contexts of privacy and data protection. Nora holds BA, LLB, and LLM (Public Law) degrees from the National University of Ireland, Galway, and was awarded a PhD in law from the University of Cambridge. Previously, Nora held the posts of Visiting Lecturer in Law at King's College London and Research Fellow and Affiliated Lecturer in Law at the University of Cambridge.

In 2019, she was appointed to the UK Home Office Biometrics and Forensics Ethics Group (BFEG) which provides independent expert advice ensuring the robustness of evidence underpinning biometrics and forensics policy development for public security within the Home Office. Nora is a member of the Board of Trustees for the British and Irish Legal Information Institute (BAILII) and an editor of leading law journal International Data Privacy Law (Oxford University Press). She is also a Senior Fellow at the University of Johannesburg and an Associate Fellow at the University of Cambridge Leverhulme Centre for the Future of Intelligence (LCFI).

Prior to her academic career, Nora was a Legal and Policy Officer for the Office of the Director of Public Prosecutions of Ireland and clerked for the Irish Supreme Court. Her work on AI, human rights, and data protection law, has been published by various leading institutions, including the BBC, The Guardian, Science, and the United Nations. She has also been an expert advisor, on matters including Brexit and cross-border data sharing, to the UK House of Lords, Chatham House, and the European Union.