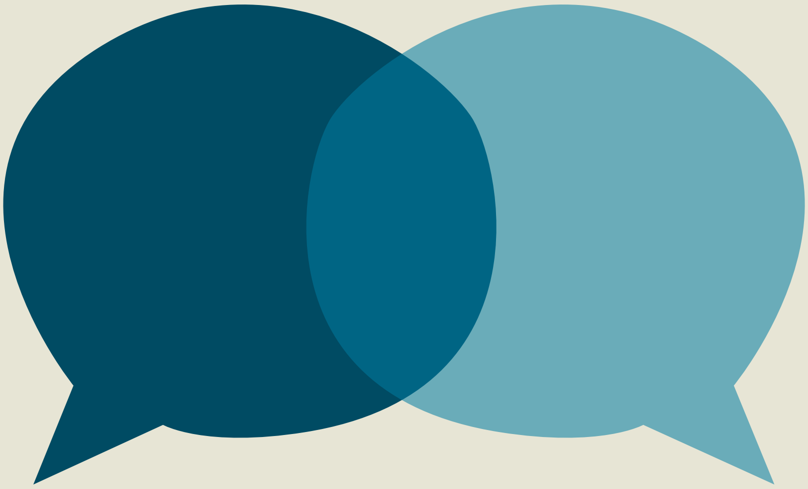

Constitutional Conversations, No. 5 of 6

Digital Citizenship

Royal Irish Academy, 30 June 2016
Report by rapporteurs Jennifer Cobbe and Louise O'Hagan

INTRODUCTION

This Constitutional Conversation on 'Digital Citizenship', the fifth in a series of six, began with the participants being guided into the reality of the 'digital world' to consider how the environment we operate in has changed significantly in recent years. The main conversational topic – 'digital citizenship' – was introduced, bringing the buzzwords 'privacy', 'security', 'data protection' and 'big data' into the conversation. It was clear that the government has major challenges around privacy, security, and data rules, as well as worries about data protection, but we were encouraged to question whether it is really about protecting the citizen. As citizens we must have interest in this – after all, it is 'our' data.

CHALLENGES OF TECHNOLOGY FOR DIGITAL NATIVES

This part of the discussion was led by two Donegal Youth Councillors who are 'digital natives', meaning that they don't know the world without the Internet and that, like many their age, they grew up online. The main focus was on the technology that young people use and the challenges that they face in doing so. The positive aspects of technology and the ubiquity of the Internet were mentioned before delving into the reality of the negative effects it is having on the younger generation.

The positives discussed were the benefits the Internet provides, particularly for those living in rural areas, where it has made it possible to keep in contact with friends and family far more easily than in the past while also providing entertainment and online shopping. The negatives were a significantly longer list, including body image pressures caused by social media and stress over how individuals are perceived, the prevalence of sexual harassment on social media (particularly experienced by young women), and catfishing (where individuals create fake profiles on social media and enter into romantic

Acadamh Ríoga na hÉireann
Royal Irish Academy

MASON
HAYES &
CURRAN

relationships online with real people). It was clear that stress can be caused by the way in which young people are expected to use the Internet. It was also mentioned that few laws are in place to protect people online, raising the question of where young people should turn for help if there is a problem. This is the reality of what the younger generation deal with, and generally speaking there is no previous knowledge that could be applied – they are the guinea pigs in this social experiment.

The question of what ownership we have of the things that we choose to publish on social media was then discussed. For the younger generation it is the norm to 'publish' their lives online – these 'digital citizens' have grown up with the Internet, constantly under pressure to post photos and tag themselves in locations. As a result of this, privacy has changed as the younger generation has grown up with a digital self where they can choose what is shown, and have learned to get 'likes' and social cachet in return for their photos and posts. Two Ps – 'public' and 'permanent' – were discussed; both should be assumed of all posts online but people often do not understand that you cannot retrieve what has been posted online. It is important to remember that what is posted online can affect job applications, and we must question how we teach the younger generation about the permanence and the public nature of what has been posted.

DONEGAL YOUTH SERVICE WEB SAFETY SURVEY

Statistics from the Donegal Youth Service web safety survey, which looked at the Internet habits of young people, were referred to. The survey revealed that females use social media twice as much as males, are under more pressure to share photos, are more likely to report abuse, and are more 'savvy' with privacy settings than males. The survey also reported that young Internet users spend on average four hours a day online, one in ten has received threats on social media, and one in three has been cyberbullied. The survey clearly highlights the need for parents to become more involved. Young people do not often have an insight into issues around Internet use. Therefore, parents need to be aware of the dangers of the Internet and to teach young people about issues such as privacy and copyright, and they need to promote knowledge and understanding of safe Internet use.

INDUSTRY EXPERT

The discussion then moved on to how we occupy ourselves with data, with contributions from an industry expert. At present we are at the heart of digital transformation and we are not sure about the implications for privacy. No one is fully aware what data is being used for, which makes it very difficult to know if it's for our benefit or not. Furthermore, data is not held on physical devices any more: it has become virtual and is often in 'the cloud'. We don't necessarily know where data goes and therefore we don't know what the threat to privacy really is, but knowing how data is used can help us understand why it is important.

THE LEGAL COMPONENT

Further discussion centred on the Irish constitution and the role it plays in relation to data. The constitution dates from 1937 and therefore says nothing about data as such, and there has been little constitutional litigation in this area to update it. The biggest limit on the state's power comes from the fundamental rights provisions. While these say next to nothing about data, Article 40.3 sets out personal rights and there has been a long trend of 'inventing' rights and shoehorning them in under this provision. One of these rights is privacy, and while case law does not directly cover data there is the ability to stop law enforcement becoming involved in private communications, which means that the state cannot access personal communications data without a warrant. There are gaps when it comes to digital citizenship, and the limitations on abuse remain unclear.

Discussion moved on to the role of EU law, which takes data protection and privacy very seriously and provides interesting and relevant material. The EU's Charter of Fundamental Rights includes a specific right to data protection in Article 8, which is distinct from the traditional right to privacy and is seen in virtually no states. Furthermore, the EU has introduced the General Data Protection Regulation (GDPR), due to come into force in 2018. This will set out clearly how data can be used and regulate the role of government, while the clear principle from European Court of Justice (ECJ) case law is that if the government is going to share data in any way, it needs to be transparent about it. The new legislation will also give citizens more control over private use of their data, allowing governments to impose penalties of up to €20 million on companies and businesses that do not comply with the GDPR.

The rights individuals have in relation to their data were then discussed. Ownership is essentially determined by copyright law and the basic rule is that whoever creates it owns it, although there are many exceptions. The restrictions on the use of information concern how it can be moved around – even when an individual does not own data they might still have rights to it.

DISCUSSION AND QUESTIONS

The discussion began with an audience member asking what 'catfishing' is, highlighting the generation gap between digital natives, who understood this term, and others. It moved on to US politics and the role of data in the last two US presidential elections. Data profiling played a particularly significant role in President Obama's two campaigns. As well as profiling, calculations of data were used to identify which fundraising strategy was most effective for each demographic. The pitch for fundraising could then be tailored to the target audience's demographic profile, and messages customised and adjusted based on what works in real time rather than through trial and error.

The question of what kind of guidance for Internet usage young people need was then discussed. Young people are not educated in privacy, Internet usage or online safety generally. This could be taught in school so that teenagers know what to do in relation to, for example, privacy settings. There was then discussion as to whether young people want to be taught specifically how to protect themselves rather than about privacy generally, with a view being expressed that teaching younger ages, especially pre-teens, about privacy and online safety is easier and more effective than attempting to do this when children enter the rebellious teenage years. The conversation moved on to whether young people should be taught how to behave online in the same way as we teach them how to act in person, i.e. should there be digital civics classes? It is important to remember that current big players (e.g. Facebook, Google) may not always be so dominant, so instead of focusing on strategies for specific sites which could be superseded by competitors, it should be recognised that teaching good ethics, manners, and common sense online is key, along with giving users the tools from a young age to enable them to exist safely online in a general sense, so that online safety becomes the norm.

What the constitution means in relation to 'digital citizenship' was then discussed. We are citizens both of Ireland and of the global digital sphere, so this may lead to jurisdictional issues. Digital citizens require digital protection, but can the state provide this? If so, should this be the state that users are in or the state where the website is based? Discussion then moved to how some companies encourage staff to have a presence on social media to promote brand awareness. There are of course dangers with developing a profile in this way. It was pointed out that for individuals the position may be particularly problematic: people feel that that there is little choice about being online as it is difficult to be active in our society without an online presence. The effect of this may be that we are all subject to the forces – both negative and positive – that an online existence brings.

The challenge of ethics was then raised: whether software and technology companies have or should have ethics advisors or ethics boards, or whether ethical issues are left to individual developers or product teams. Do the ethical decisions (or non-decisions) necessarily taken in many aspects of the industry match the expectations of their customers, the users of their products, and their trading partners? What is the role for the states in this?

The conversation moved to comparing the 'tyranny of data' in the private sector with the tyranny of not having access to data in the public sector. The public sector often has strict restrictions on what can be done with data and there are often limits on data sharing between public sector bodies. This creates a double standard whereby there are few protections on the use of data in the private sector but many in the public sector. Perhaps the issue is not one of data sharing but of governance – sharing does happen to some extent in the public sector and can provide benefits to government, so rather than continuing to restrict it we perhaps need to focus on allowing data sharing and regulating it under a proper framework with privacy issues at the centre.

The discussion was then widened to include big data, the Internet of things, and algorithmic government. It was mentioned that systems that learn from the behaviour of people may have the potential to reflect the true nature of humanity – although it is difficult to incorporate into data the societal and cultural standards that temper some of the harsher elements of human nature. The conversation then focused on algorithms rather than data, discussing how in many US jurisdictions judges are using sentencing databases. Using these systems, convicted people are profiled and their sentence is tailored to what the computer determines their likelihood of reoffending is, based on historical data. The example was also given of a chatbot that challenges parking tickets, taking in information from the user and determining the likelihood of a successful challenge based on experience gained in previous challenges, which has been hugely successful. A further example was predictive policing, which profiles individuals and determines, based on historical data, the likelihood of them offending, and which is beginning to be rolled out in some parts of the US, China, and Russia. The discussion emphasised that it is important to think about how the state can use data rather than thinking only about the data itself.

CONCLUDING REMARKS

The general conclusion was that the word 'privacy' is fuzzy and ill-defined and that we often have little or no idea what we are talking about when we refer to the right to privacy, particularly in relation to data. Indeed, the discussion raised an abundance of questions that may never be answered. The aftermath of Brexit lingered throughout the conversation, and in closing it was suggested that maybe there should be a vote for digital citizens to leave or remain in the online world.

Convenors: **John Morison** MRIA
Andrew Power, Dún Laoghaire Institute of Art, Design and Technology
Chair: **Noreen O'Carroll,** Royal College of Surgeons in Ireland
Panellists: **Oisín Tobin**, Senior Associate, Mason Hayes & Curran
Anthony Behan, IBM
Aoife Gillespie, Donegal Youth Councillor
Hannah Healy, Donegal Youth Councillor

ATTENDEES

Ken Breen	Gallagher Shatter Solicitors
Tara Casey	Gallagher Shatter Solicitors
Colleen Connolly	Accenture
Richard Corbridge	Health Service Executive
Elizabeth Fitzgerald	Technology and Commercial Law
Connor Fitzmaurice	Office of the Chief Government Information Officer
Helen Gibbons	Noel Smyth & Partners
Adam Harkens	Queen's University Belfast
Deirdre Haslett	Member of the public
John Haslett	Member of the public
Liam Heaphy	Maynooth University
Kate Higgs	William Fry
Laura Howard	Trinity College Dublin
Caitriona Keane	Chief State Solicitor's Office
Rónán Kennedy	NUI Galway
Killian Keogh	Noel Smyth & Partners
Panagiotis Loukinas	Queen's University Belfast
Paul McCusker	Letterkenny Institute of Technology
Aisling McGowan	Noel Smyth & Partners
Slawomir Norberczak	Polish media journalist
Daragh O Brien	Castlebridge Associates
Aileen O'Carroll	Digital Repository of Ireland
Patricia O'Hara	National Statistics Board
Conor O'Leary	Noel Smyth & Partners
Maria O'Loughlin	Health Service Executive
Anthony O'Neill	Eir Ireland
Hilary Treacy	Barbican, Data Protection Services
Lisa Underwood	Houses of the Oireachtas