Creating a 'Digital Bill of Rights':
Why do we need it, and what should we include?

Introduction

This paper sets out our ideas for a future Digital Bill of Rights. It is a preliminary proposal only, for further co-creation with industry, academia, and civil society.

This process of consultation will help define the approach we should take to these issues in any future coalition negotiations. It will also inform our position with regard to the forthcoming EU Data Protection Regulation.

What is the purpose of the Bill?

There is no comprehensive piece of law that sets out our digital rights in one place. Where such rights do exist, they have developed, in a piecemeal fashion, as a result of human rights law, UK legislation and EU directives.

Since the passage of the Data Protection Act in 1998, there have been huge technological advances. These include a tectonic shift in the way we interact socially and an explosive growth in data creation. These changes have brought enormous social and economic benefits, but they have also created an array of opportunities for the misuse of personal data, whether by public authorities, criminals, or commercial interests.

The time has come to set out the fundamental rights and liberties that will protect us and enable us to thrive as confident citizens and consumers of the digital world. The time has come for a Digital Bill of Rights.

The Bill has four aims:

- Ensure that the civil and human rights that apply in the physical world also apply online
- Establish the key rights that are particular to the digital sphere
- Ensure greater transparency around the ways in which government and private companies use personal data
- Protect and empower citizens to take control of their own data and to make informed choices about their digital lives.

Relationship to other proposals

The Bill will incorporate the core principles set out by the iRights coalition (http://irights.uk), the WebWeWant campaign (https://webwewant.org), and the Reform Government Surveillance coalition (https://www.reformgovernmentsurveillance.com).

The language and policy objectives of the Bill will be affected by the forthcoming EU Data Protection Regulation, which is intended to address some of these issues across borders using a multinational framework; exactly the approach required for an internet that knows no borders.

THE PROPOSALS

1. Control of personal data

THE BIG IDEA: Personal data[1] should, in principle, be subject to the control of the individual to whom it refers[2].

In practice, this would mean:

- Everyone has the right to view, correct, and (where it is appropriate and proportionate to do so) delete their personal data, whether it is held on a public or private computer system.

- Personal data held by public or private bodies must be made available on request to the individual to whom it refers, in an open digital format.

- In principle, personal data should only be acquired, stored or processed with the explicit consent[3] of the individual.

- Where data that includes the personal data of individuals is accessed and used by government, industry or research organisations, the details of that use (by whom, and for what purpose) should be recorded and published as open data.[4]

- Where government or its agencies accesses an individual's personal data without their consent, that individual should be notified in a timely manner where it is safe to do so.

And why is this so important?

As Liberal Democrats we believe in empowering citizens. Control of our personal data should be in our hands, not in the hands of big business or the government.

[1] 'Personal data' is defined in the Data Protection Act 1988 as "data which relate to a living individual who can be identified, (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

[2] Exceptions to this principle may include the assignment of rights by way of contract, and data collected by the state for specific purposes authorised by statute.

[3] Explicit consent means that it is freely given, specific and informed, and occurs by way of an affirmative action on the part of the consumer.

[4] 'Open data' is data that anyone can access, use and share. Requiring the publication of details of requests for access to and use of an individual's personal data as open data is an important transparency mechanism. The Department for Education, for example, publishes details of requests for access to the National Pupil Database: https://www.gov.uk/government/publications/national-pupil-database-requests-received

2. Control of user content

THE BIG IDEA: Everyone should be able to access, edit or remove any online content which they themselves have created.

In practice, this would mean:

- Internet-based services should provide a means by which users of the service can view, edit or remove content which they have posted on the service. This would not extend to publicly available content which has been reproduced or shared by other users.

- Where content refers to an individual but was not created by them, online services should follow a Code of Practice by which that content can be corrected, in a timely manner, where it is inaccurate or defamatory. The Code of Practice will be developed in consultation with industry and civil society groups to ensure strong protections for freedom of speech.

And why is this so important?

As Liberal Democrats we believe in fostering creativity and empowering people to shape their own identities. That's why content that we have chosen to put online (whether that's a tweet, an image or a blog post) should be under our control.

3. Limits on the use of personal data

THE BIG IDEA: No public body is to collect, store or process personal data without statutory authority or explicit consent.

In practice, this would mean:

- Legislation, regulations and guidance pertaining to the collection, storage, encryption, use, and sharing of personal data by government or its agencies must clearly set out the purpose of that activity and the rules by which it should operate.

- Legislation authorising the collection and use of personal data should be subject to periodic post-legislative scrutiny in order to assess whether the collection and use is still justified, and to take account of the impact of developments in technology.

- Public bodies should publish annual transparency reports setting out the type of data, the number of data subjects, and the quantity of data being collected. Public bodies would be subject to periodic auditing of data collection to ensure compliance.

And why is this so important?

As Liberal Democrats we believe that authority in a democracy derives from the people. Government and public bodies should only hold information about us where it has the authority from Parliament to do so.

4. A free and open internet

THE BIG IDEA: An open and neutral internet is essential for open government, good democracy, a strong economy, connected communities and diversity of culture.

In practice, this would mean:

- The Ministerial Code should require government Ministers to uphold the free, open, multi-stakeholder internet in both their domestic and international dealings.

- A Cabinet-level Minister should be appointed to direct overall policy development in relation to digital technologies and the internet, and to ensure cross-departmental collaboration and cooperation. He or she should regularly brief ministerial colleagues, the media and the public to explain current policy, new developments, and legislative requirements, as well as to explore opportunities for innovation in government and public services.

And why is this so important?

As Liberal Democrats we believe in an open society where everyone is free to fulfil their potential. The free, open internet embodies that principle. As Vint Cerf, one of the early pioneers of the internet, has said, "When the internet was conceived in the early 1970s, the notion of openness lay at the heart of its architecture, philosophy and technical protocols"[5]. Similarly, "the institutions that were created to cater to the evolution of the internet were open, bottom-up and inclusive"[6]. The free, open internet is a precious achievement and government should have a responsibility to protect it.

5. Freedom of speech

THE BIG IDEA: The right to free expression applies online just as it does in the offline world.

In practice, this would mean:

- Government has a responsibility to uphold the right to free expression online, which extends to expression in all its forms, including text, videos, audio recordings, and other forms of public communication.

- Government has a responsibility to defend the free press, including the rights of journalists and citizen journalists to express their views freely online. This responsibility should specifically extend to intermediaries (i.e. organisations that host but do not author the material), which can be particularly prone to pressure to remove lawful content.

[5] http://home.web.cern.ch/cern-people/opinion/2013/04/open-internet-and-web
[6] Ibid

- Government has a responsibility to ensure that the criminalisation of any speech is limited to what is necessary and proportionate in a free and democratic society. In particular, the criminal law should be targeted at protecting the physical integrity and security of individuals, and not the protection of moral attitudes, beliefs, or viewpoints.

- Outdated laws which focus on the method of communication rather than the content or impact of the communication should be repealed or replaced by coherent and consistent legislation.

- Any request made by government or its agencies to censor online speech must have a clear statutory basis in law, with recourse to the courts in the event of a dispute. Lawful speech must not be censored by the government, either through formal or informal processes.

- All instances (whether formal or informal) of government-initiated censorship online (including network-level blocking of content hosted overseas) must be recorded and published in annual transparency reports, including as open data.

And why is this so important?

As Liberal Democrats we believe that freedom of speech is a fundamental and inalienable right. As new methods of communication emerge, we need to guard against new forms of censorship.

6. Privacy

THE BIG IDEA: People have the same rights to privacy in their telecoms and their online lives as they do in the offline world.

In practice, this would mean:

- Government has a duty to uphold the privacy of citizens in their telecommunications and in their digital lives, and to ensure that the necessary frameworks are in place to protect personal data. Exceptions to this principle must be clear, prescribed by law, and subject to oversight.

- Privacy should only be invaded by public authorities where there is reasonable suspicion of criminal activity or where it is necessary and proportionate to do so in the public interest, and with appropriate oversight by the courts.

- Any proposal for legislation which could impact on online privacy should be referred by Ministers to the appropriate advisory bodies (the Privacy and Consumer Advisory Board, Privacy and Civil Liberties Board, and the Information Commissioner) for advice at an early stage.

- There should be no unnecessary collection or storage of data in a form that can be used to identify individuals. Public and private bodies must take steps to ensure that data is anonymised or aggregated in such a way that individuals cannot be easily identified[7].

And why is this so important?

As Liberal Democrats we believe that everyone has the right to respect for their private and family life. While it is true that many people choose to share details of their private lives with their contacts on social media, the default position should be that personal data is private unless individuals consent to share it, or the public interest in disclosure outweighs the interests of the individual. We should not allow technological changes to lead to an erosion of privacy.

7. Surveillance

THE BIG IDEA: State surveillance of the internet must be the exception rather than the norm, and must only take place where it is clearly justified for the protection of the public and in accordance with the fundamental principles of necessity and proportionality.

In practice, this would mean:

- A complete review of all existing surveillance legislation, including refining or modifying distinctions between: internal and external communications; different types of data; communication formats; retention and access[8]. In future, the emphasis in legislation should be on the nature and level of intrusion, rather than the method of obtaining data or its location when intercepted.

- There should be no blanket collection of UK residents' personal communications by the police or the intelligence agencies.

- Government should not require Communications Service Providers to retain any bulk data for law enforcement or intelligence purposes unless it can demonstrate that it is strictly necessary and proportionate to do so in order to protect the public from crime. The process for any such retention must be clearly set out in law, time-limited, and subject to public scrutiny and proper Parliamentary oversight.

- Communications Service Providers should not be required to collect third-party communications data for non-business purposes.

[7] For example, by blurring faces in live CCTV feeds or collating web browsing data for advertising purposes according to groups who share similar characteristics.

[8] Liberal Democrats in government have already set this review process into motion. The Independent Reviewer of Terrorism Legislation, David Anderson QC, is currently conducting a review of the Regulation of Investigatory Powers Act under the terms of the Data Retention and Investigatory Powers Act (DRIPA) 2014. The product of this work, together with report of the independent expert panel set up by the Royal United Services Institute, will feed in to a further government and parliamentary work leading up fresh legislation prior to the expiry of the DRIPA powers in December 2016.

- Access to metadata, live content, or the stored content of personal communications must only take place where there is reasonable suspicion of criminal activity, or to prevent threats to life.

- The acquisition of communications data which might reveal journalists' sources or other privileged communications should be subject to judicial oversight and authorisation. Journalists should have the opportunity to address the court before authorisation is granted, where this would not jeopardise the investigation.

- The police and intelligence agencies must not obtain data on UK residents from foreign governments that it would not be legal to obtain in the UK under UK law.

- Any government request for access to personal data stored in another legal jurisdiction should take place within a prompt, lawful and transparent international framework.

- Surveillance powers must not be extended without primary legislation from Parliament.

- All government surveillance must be subject to oversight which is independent, informed, transparent and effective.

- Government must publish annual transparency reports, including as open data, setting out comprehensive and detailed information on the use of powers to access personal data by law enforcement and the intelligence agencies, and other public bodies. There must be a corresponding right for individual companies or organisations which have received surveillance warrants or notifications to publish similar transparency reports.

And why is this so important?

As Liberal Democrats we believe that surveillance without suspicion is alien to our values. The intelligence agencies do vital work and deserve our support. But unless surveillance is properly regulated according to a clear set of principles that enjoy public support, it will undermine confidence in both the security services and the integrity of the internet.

8. Consumer rights

THE BIG IDEA: Consumers have the same rights to fairness and transparency online as they do in the offline world.

In practice, this would mean:

- It should continue to be an offence to acquire personal data and sell it to third parties without informed consent or legal authority.

- Where personal data that is not necessary for the provision of a service has been collected without the informed consent of the individual, there should be a legally enforceable right to have that data deleted in a timely manner.

- Privacy policies and terms and conditions of online services, including apps, must be clear, concise, and easy for the user to understand, so that any consent that they give in relation to the use of their data is properly informed.

- The relevant government departments or regulators should work with industry to develop standardised wording for privacy policies, to increase transparency and reduce complexity, and assist companies in following and applying the Data Protection Act principles.

- Terms and conditions for online services targeted at children and young people must be fair to those they are aimed at and be written in a way that makes clear the current and future consequences of their agreement to provide their personal data and content.

- Regulatory bodies should have the power and resources to review the fairness of such privacy policies and terms and conditions. Where terms and conditions are found to be unfair, consumers should have a right to compensation or other appropriate redress if they are negatively affected.

- Government should provide the necessary information and guidance on these matters to enable and empower any individual to fully understand and exercise their rights in relation to these matters.

And why is this so important?

Liberal Democrats believe in a strong economy and a fair society. As consumers, we need to have confidence that our rights are protected, whether our purchases are made online or on the high street.

9. Encryption

THE BIG IDEA: Strong cyber-security is the basis of a strong digital economy: individuals, businesses and public bodies have the right to use strong encryption to protect their privacy and security online.

In practice, this would mean:

- Government has a responsibility to uphold and facilitate the strongest security standards online and should not seek to weaken encryption or obstruct the availability of encryption technologies.

- Surveillance legislation and policies must take into account any potential impact on the digital economy.

- Basic cyber-security means that encryption of data should be the norm, rather than the exception.

- No request should be made to decrypt content unless it is necessary and proportionate to do so for purpose of protecting the public.

- Decryption should only take place on a case-by-case basis, and companies should not be expected to hand over to Government the encryption master-keys.

And why is this so important?

As Liberal Democrats we believe that a strong economy needs a vibrant, robust and secure digital sector. Businesses must be able to protect their communications, their intellectual property and their customers' data from intrusion; and individuals and families need to have confidence that their private information, photos and conversations are not vulnerable to hackers.

10. Right to unrestricted internet access

THE BIG IDEA: The ability to access information on the internet is an essential right that supports the ability of citizens to be informed and engaged in public life. It is also vital for the proper functioning of public services, and helps to ensure the free flow of information that underpins the functioning of markets. The overarching objective of a neutral network means that there can be no unfair discrimination against content or users.

In practice, this would mean:

- The Government has a duty to ensure, by promoting effective competition, that citizens and consumers have universal and affordable access to the internet.

- The Government should treat access to the internet as a basic utility in future legislation and policies, with specific provision made for vulnerable consumers, similar to other utility legislation covering water, gas and electricity.

- Local authorities should provide free internet access points, for example in public libraries.

- Access to an unrestricted internet is a right that can only be infringed by legitimate security reasons, for example where a court has determined that it is necessary to do so for the prevention of serious crime. Governments must not otherwise take steps to restrict or throttle citizens' access to the internet.

- The principle of net neutrality should be defined and enshrined in a Code of Practice with a statutory underpinning, so that internet service providers do not filter lawful content without their users' active agreement, nor strike deals with content providers which result in them taking up significant bandwidth and distorting the content available to users.

- Exceptions to the general net neutrality rule must be clearly defined in the Code of Practice, which will allow such exceptions when it is in the collective interest of users; i.e. sufficient bandwidth for priority for voice communications and video on demand, or enabling the effective development or operation of the Internet of Things.

- The Code of Practice and any associated technical guidance will be developed by the Government in close consultation with industry, consumer advocacy groups and relevant interested parties.

- The Government should not mandate the filtering of lawful online content. Customers should be given the choice of whether they want to have certain material (e.g. pornography) blocked when they connect to the internet, but service providers should not present their users with the default assumption that they want legal content to be blocked.

And why is this so important?

Liberal Democrats we believe in a society that is fair, free and open. As citizens and as consumers we are all entitled to the same ability to access information online.

11. Right to access and use publicly funded data and research

THE BIG IDEA: The first 25 years of the internet was a Web of documents. The next 25 years will see the evolution of the Web of data. Data that is created and maintained by government using public funds should be accessible to the public to use and share. The outputs of publicly funded research should also be published under an open license, fostering innovation and knowledge sharing.

In practice, for non-sensitive and non-personal data, this would mean:

- Data created by government departments and bodies should be published as 'open by default': licensed for anyone to access, use and share.

- Data created as part of publicly procured services should also be published under an open license.

- Organisations and individuals undertaking research and development using public funds should publish the results of their initiatives under an open license.

And why is this so important?

As Liberal Democrats, we believe the state has a responsibility to disperse power and foster creativity. We are committed to ensuring that public services are responsive to the people they serve, and that policy making is based on good evidence. It is therefore vitally important to unlock the value that lies in public datasets, so that consumers can benefit from the development of innovative products and services, and citizens can hold their public services to account.

12. Digital literacy

THE BIG IDEA: Children and young people should be able to enjoy the benefits of digital technologies without compromising their safety or privacy.

In practice, this would mean:

- Digital literacy should be considered a core pillar of the national curriculum, alongside numeracy and literacy.

- Schools should equip children and young people with the skills and confidence they need to use and critique digital technologies.

- Companies which operate in the online sphere should have a duty to provide age-appropriate policies, guidance and support to children and young people who use their services.

- Children and young people should be confident that they will be protected from illegal practices and supported if confronted by troubling or upsetting scenarios online. To support this objective, Government should support a variety of civil society groups who are able to help young people navigate the internet and any challenges they face.

- Our national curriculum and our education system should cover and address basic life questions, to ensure that the internet is not the only source of information on sex and relationships.

And why is this so important?

As Liberal Democrats we believe that children and young people need to have the opportunity to reach their full potential. That's why it is so important to teach digital literacy and skills, to ensure that young people are able to take control of their digital identities.

13. Enforcement of digital rights

THE BIG IDEA: Anyone whose digital rights are breached has the right to complain to a competent authority and to have that complaint acted upon.

In practice, this would mean:

- The Information Commissioner should have the power to proactively audit any body which processes personal data, without the consent of that body.

- The Information Commissioner must be adequately funded to ensure that their regulatory enforcement powers are neither hampered nor unduly restricted by a lack of resources.

- Breach of data protection law should result in a commensurate fine for the body concerned, disciplinary action for employees, and/or compensation for the individual(s) affected.

- Specific provision should be made to allow for individuals to use the small-claims court procedure for seeking a remedy or redress for breaches of digital rights.

- The Information Commissioner should have the power to compel the release of data created by government, or in the course of publicly-procured services, as open data where it is in the public interest to do so.

- The theft or illegal sale of personal data resulting in loss of privacy or other harm to individuals should result in penalties up to and including a prison sentence.

And why is this so important?

As Liberal Democrats we believe in liberty, justice and the rule of law. For everyone to have confidence in the system, there should be appropriate and proportionate remedies available to penalise those who breach our rights online.