The Contract for the Web: A new "Global plan of action to make our online world safe and empowering for everyone"

DISCUSSION PAPER

Should the Privacy Foundation NZ endorse the "Contract for the Web"?

10 December 2019

Recently Sir Tim Berners-Lee launched an initiative known as the "Contract for the Web" as a shared global plan to protect a free and open web that works for the public good.

The next step includes a push for more civil society organisations to endorse the plan as the project carries on to propose new global standards for areas of policy where they currently don't exist and to develop measurement and accountability mechanisms.

The Privacy Foundation NZ Committee seeks members' views on whether the Foundation should endorse the Contract for the Web. This paper is the first step in this discussion which will initially be carried on electronically using email, the website and the Foundation's twitter account.

Throughout the paper certain questions are posed in italics. These are the sort of matters that the Committee will seek to answer and on which members' views will be welcomed.

We encourage interested members to read this paper, visit the Contract for the Web website https://contractfortheweb.org/ and actively participate in the discussion on the Foundation's twitter account @PrivacyFdn_NZ. We also welcome emails.

Background

> *"Half of the world's population still can't get online. For the other half, the web's benefits seem to come with far too many unacceptable risks: to our privacy, our democracy, our health and our security.*
> *"Now for the first time ever, we have a global plan of action — the Contract for the Web — created by experts and citizens from across the world to make sure our online world is safe, empowering and genuinely for everyone."*
> From the Contract for the Web website

In November 2018, Sir Tim Berners-Lee announced a project to build a new Contract for the Web that would bring governments, companies and citizens together around a shared set of commitments to build a better web. In January 2019, over 80 signatories to the contract principles debated and negotiated the full details and commitments to be outlined in the full Contract. That process was informed by a public consultation with input from more than 600 people, including

policy experts. In July 2019, the first draft text of the Contract for the Web was published. The completed version was released in November.

More details are available at: https://contractfortheweb.org/

The Contract for the Web

The initiative describes itself as "A global plan of action to make our online world safe and empowering for everyone".

At its heart are 9 principles (1-3 directed to governments, 5-6 to companies, and 6-9 to citizens):

1. Ensure everyone can connect to the internet
2. Keep all of the internet available, all of the time
3. Respect and protect people's fundamental online privacy and data rights
4. Make the internet affordable and accessible to everyone
5. Respect and protect people's privacy and personal data to build online trust
6. Develop technologies that support the best in humanity and challenge the worst
7. Be creators and collaborators on the Web
8. Build strong communities that respect civil discourse and human dignity
9. Fight for the Web

The website elaborates upon these. For example, privacy principles 3 and 5 are directed to governments and companies are set out below. As can be seen those two high level principles split into 6 sub-principles which in turn cascade into 24 specifics.

Question 1: Is privacy principle 3, and its 3 sub-principles something the Foundation can support?

Question 2: Is privacy principle 5, and its 3 sub-principles something the Foundation can support?

Members are encouraged to visit the project's website which explains all the principles in detail.

The initiative also contains principles that are focused upon social values and interests other than privacy. Anyone familiar with privacy law and practice, as many Foundation members will be, realise that privacy cannot be considered entirely in a vacuum and must reckon with other values and interests that touch upon information handling.

There are issues for the Foundation in endorsing an action plan that goes beyond issues simply of privacy. The Committee will be carefully considering this aspect and welcomes members views on the general issue and the specifics of all the principles.

In many areas the Foundation will have no difficulty in expressing support for a value that is not purely a matter of privacy. Examples might include support for, say, the rule of law, human rights or accountable public bodies. In some other cases, the Committee might wish to avoid taking a stance on a matter of political or public controversy where it is so remote from privacy that we would be unable to claim expertise.

At a general level the Committee will wish to consider whether the full scheme of principles are ones that lie in areas of relevance to the Foundation. Of course, the principles in this initiative all touch upon the internet, a medium central to many contemporary privacy issues. One view may be that in terms of risks and benefits to individuals the information world is interconnected that the Foundation should not be unwilling to take a position on some issues, such as web-accessibility, that on first glance seem remote from privacy. Another view may be that we must stick very closely to our area of core expertise. We welcome hearing members' views.

In addition to considering a matter of general approach it is also necessary to look at the detail of the non-privacy principles to check that there is no content that the Foundation would be opposed to and that generally speaking we are comfortable with those principles. We welcome members drawing the Committee's attention to aspects that should be considered carefully.

Question 3: At a general level should the Foundation endorse a set of principles that go beyond purely privacy issues into other proposals to 'make the online world safe and empowering for everyone'? What should be the key considerations for the Committee in your view?

Question 4: Should the Foundation be comfortable endorsing principles 1, 2, 4, 6, 7, 8 and 9? If you see areas of possible concern, please highlight these for the Committee and explain why.

What is the purpose of endorsement?

This is new territory for the Foundation so we cannot be sure how useful our endorsement will in practice be. However, in principle, we hope that any endorsement:

- Will show solidarity between the Foundation and others working internationally on web issues and possibly create new connections and contacts that may be useful in the Foundation's work.
- Will be valued by the project and, in a small way, help the principles gain international traction.
- The endorsed principles will be useful in domestic campaigning for better privacy law and practice.

The Foundation's Committee will further consider the matter at its meeting in February.

Discussion paper prepared by Blair Stewart, Committee member and co-convener of international working group.

Annex: Principles 3 and 5 on Privacy

Principle 3

Respect and protect people's fundamental online privacy and data rights

So everyone can use the internet freely, safely, and without fear

---

1. By establishing and enforcing comprehensive data protection and rights frameworks

– to protect people's fundamental right to privacy in both public and private sectors, underpinned by the rule of law. These frameworks should be applicable to all personal data — provided by the user, observed or inferred — and include:

1. An appropriate legal basis for data processing. Where the legal basis is consent, it must be meaningful, freely given, informed, specific, and unambiguous.
2. The right of access to personal data, including to obtain a copy of all personal data undergoing processing by an entity, so long as such access does not adversely affect the rights and freedoms of other users.
3. The right to object or withdraw from processing of personal data, including automated decision making and individual profiling, subject to explicit limits defined by law.
4. The right to rectification of inaccurate personal data, and erasure of personal data, when not against the right of freedom of expression and information or other narrow limits defined by law.
5. The right to data portability, applicable to the personal data provided by the user, either directly or collected through observing the users' interaction with the service or device.
6. The right to redress through independent complaints mechanisms against public and private bodies that fail to respect people's privacy and data rights.

---

2. By requiring that government demands for access to private communications and data are necessary and proportionate to the aim pursued,

– lawful and subject to due process, comply with international human rights norms, and do not require service providers or data processors to weaken or undermine the security of their products and services. Particularly, such demands should always be:

1. Made under clearly defined laws subject to a competent and independent judicial authority that includes fair avenues for redress.
2. Restricted to those cases where there is a legitimate public interest defined in law.
3. Time-bounded, and not unduly restricted from disclosure to affected individuals and the public.

---

3. By supporting and monitoring privacy and online data rights

– in their jurisdictions, particularly:

1. Minimizing their own data collection to what is adequate, relevant, and necessary to achieve a clearly specified public interest.

2. Requiring providers of public services and private actors to comply with existing relevant legislation and supporting strong enforcement —including administrative penalties— by independent, skilled, empowered, and well-resourced dedicated regulators.

3. Mandating public registers to promote transparency of data sharing and/or purchase agreements in public and private sectors for profiling purposes, as well as for significant data breaches that are of public interest, to make users aware of when and how their data could be exposed.

4. Requiring regular data security and privacy impact assessments, providing independent and transparent oversight of the assessments and independent audits for public and private sectors, and enforcing when appropriate.

Principle 5

Respect and protect people's privacy and personal data to build online trust

So people are in control of their lives online, empowered with clear and meaningful choices around their data and privacy

---

1. By giving people control over their privacy and data rights, with clear and meaningful choices to control processes involving their privacy and data, including:

1. Providing clear explanations of processes affecting users' data and privacy and their purpose.

2. Providing control panels where users can manage their data and privacy options in a quick and easily accessible place for each user account.

3. Providing personal data portability, through machine-readable and reusable formats, and interoperable standards — affecting personal data provided by the user, either directly or collected through observing the users' interaction with the service or device.

---

2. By supporting corporate accountability and robust privacy and data protection by design,

– carrying out regular and pro-active data processing impact assessments that are made available to regulators which hold companies accountable for review and scrutiny, to understand how their products and services could better support users' privacy and data rights, and:

1. Minimizing data collection to what is adequate, relevant, and necessary in relation to the specified, explicit and legitimate purposes for which the data is processed, and limiting further processing of the data to what is compatible with those purposes.

2. Supporting independent research on how user interfaces and design patterns ☐—including processes for obtaining consent and other relevant user controls☐— influence privacy outcomes, and ensuring those follow good privacy practices.

3. Enabling controls over how personal data is collected and used ☐—including third-party and persistent tracking☐— that could be reviewed and adjusted at the user's convenience, and making those easy to locate and use.

4. Developing and adopting technologies that increase the privacy and security of users' data and communications.

---

3. By making privacy and data rights equally available to everyone,

– giving users options to access online content and use online services that protect their privacy, and:

1. Providing dedicated and readily available mechanisms for individuals to report adverse privacy and data protection impacts directly linked to the company's operations, products or services — which the company should address and mitigate as required by law.
2. Promoting innovative business models that strengthen data rights, respect privacy, and minimize data collection practices.
3. Providing clear and understandable privacy policies and consent forms, where the types of personal data processed are listed, and the purposes of data collection and use are explained.
4. Clearly and effectively communicating any updates and changes regarding privacy policies, as well as changes to products and services where the impact on individuals' privacy rights is not in line with the privacy policies in place.