May 24th 2019

Policy Brief -

Principles for Responsible Data Handling

Internet Society

Policy Brief - Principles for Responsible Data Handling

Responsible data handling means applying ethical principles of transparency, fairness and respect to how we treat the data that affects people's lives. It can protect our privacy and autonomy and build the trust needed for digital innovation to flourish in ways that benefit everyone.

Introduction

More and more of our activities generate data which is collected and used in ways we don't see and can't control. While the data is used for analytics and targeted advertising that can potentially improve services enhance our experience as consumers or public service users, its use can also undermine privacy, autonomy, and trust in the digital economy as a whole.

Simply put, responsible data handling means going beyond "can we do this?" and asking "should we do this?". Its aim is to protect privacy and autonomy and maintain trust in the Internet, allowing innovation to flourish. Responsible data handling co-exists with data protection rules and is a guide on how to act when these rules do not exist or are patchy, or in situations the rules did not anticipate. However, "should we do this?" can be a question that organisations need help to answer. This paper sets out ethical principles and recommendations to provide that help.

Why do we need to handle data 'responsibly' when there are often existing privacy and data protection rules?

- There are strong short-term financial motivations to over-collect and monetize data, but this can harm individuals' interests and leave them feeling powerless and resentful, corroding overall trust. Data handling that undermines trust damages sustainable economic growth.
- Technological innovation generally moves faster than policy development. Data protection rules cannot foresee every single use of data, and enforcement may be inconsistent or even absent. Data-handlers need to use their judgement, and ethical principles show how to do this.
- Just following the rules without thinking encourages a 'box-ticking' risk and compliance culture that misses the underlying goals of data protection and fails to consider how negatively individuals may view apparently legitimate uses of their data.
- Data protection doesn't cover everything. People can be impacted by data-processing that is not specifically *about* them but which *affects* them. For example, users of certain laptops may be charged more for consumer products; airlines may charge higher fares to those who have browsed prices before; and people with names associated with certain ethnic or racial groups

may find they are refused credit, housing or even given longer prison sentences. None of these instances of harmful data handling necessarily breaks data protection rules, but all of them feel unfair to many and undermine trust in data handling as a whole.

Privacy and data protection rules aim to protect individuals' interests, but data-handlers can still do things that are legal but unfair, manipulative or even exploitative. Trust is vital to citizens' willingness to use government services and to engage with the Internet economy as a whole. It is much harder to restore than it was to build in the first place. Responsible data handling goes beyond the legal baseline to embed ethically-based best practices that protect people's interests and build their trust.

Challenges

People don't just *feel* they are losing control of their data; they *are* losing control of their data. Worse, unethical uses of individuals' data can cause real harm. Recent news stories include:

- Household consumer electronics record and forward people's conversations;
- Social media mobile phone apps collect the personal data of users' family and friends without their consent;
- A fitness tracker publishes maps of runners' daily routes, including soldiers in military bases and victims of stalking and domestic violence;
- A dating app shares the HIV status of its users with commercial third parties;
- Individuals deported from a country of which they are citizens, because the authorities fail to exercise due diligence when checking citizenship.

One lesson from several of these examples is that IoT plays an increasing part in lessening people's sense of control over information about them and their lives. Another is that responsible data handling is not just a matter of *refraining* from bad practice: it also implies *positive* obligations (for example, to ensure that you exercise due diligence when using personal data as the basis for decisions that affect others).

In consumer environments, where harm is considered lesser, but where customers might be expected to exercise their choice, 63% of Internet users expressed high levels of distrust in social media, search and tech companies.[1] Individuals feel increasingly powerless in the face of widespread unethical data use because of:

[1] 2018 CIGI survey on Internet Security and Trust

- Lack of transparency about how their data is handled, and by whom, which also means negative future consequences can't easily be traced back and fixed;
- Lack of alternatives to the data-hungry firms that dominate the consumer experience; poor data portability may also be a factor in increasing users' sense of being locked in to a particular platform or service.

The distrust many feel in both public and commercial digital services is growing, and recent developments in several countries show that what is at stake is not just trust between people and companies or governments, but the confidence of citizens in our wider information and democratic systems. Responsible data handling is a single but essential part of ensuring that technology serves everyone's broader and long-term public interests.

Key Considerations

The Internet Society believes that when people can *see* that data about them is responsibly and respectfully used, there is a trust dividend which can not only build competitive advantage, but also enhance the trustworthiness and sustainability of online services, and of the broader online and societal environment as a whole.

For Governments

Governments have a positive duty to ensure the privacy, autonomy and security of their citizens in an increasingly digital world. This means establishing and enforcing clear rules, leading by example on responsible data handling, and encouraging data handlers to consider the impact of their choices on everyone affected by them.

As data handlers themselves, governments are custodians of often sensitive data about citizens. If people don't trust online public services, it will not only be costly to provide manual or face-to-face alternatives, but new initiatives like smart cities may fail.

As policymakers and regulators, government actors should support and resource effective regulation and enforcement, apply consumer law on deceptive or unfair practices and business models where necessary, support education and awareness to stimulate consumer demand for data-respectful

services, and, especially, ensure that the costs and risks of bad practices are born by organizations, not by individuals.

Looking outward, governments need to set the standard for secure and respectful data use, and to wield their influence as buyers of products and services to influence others to handle data responsibly. Governments can provide incentives for responsible data handling through their own procurement requirements, but also through credible certification schemes, stimulating a market for independent privacy audits, applying penalties for unlawful practices, violations and breaches, and allowing insurers to take certification and good practice into account when something goes wrong[2].

For Private Sector Data-Handlers

Many organizations say they "take the privacy of our customers very seriously", but if challenged to prove it would not be able to show that they have done more than fulfil basic legal requirements. With growing consumer cynicism about consent practices and lengthy privacy policies that minimize company liability rather than protecting privacy, there is a competitive benefit to companies that can show how they put clear ethical principles into practice.

Responsible data handling deepens trust and can be a competitive advantage for attracting customers, including commercial and government clients. Setting a high ethical bar, so that the organisation must actively minimize the collection of data and carefully evaluate its use, can prevent the development of a "check-box" culture that leads to breaches and unwelcome surprises.

For example, if the analysis of a new digital service's use-cases and impact is too narrowly scoped, it may fail to consider potential impacts on a wide range of users, particularly vulnerable ones. When these impacts become publicly known, the adverse effects often come as a surprise to the service-provider. But by then, the reputational damage is done.

Responsible data handling means not just minimizing data collection and fine-tuning practices, but also re-positioning yourself and asking;

- If I was a user of this service, would some of its uses of data surprise me? Dismay me?

[2] This is a principle set out in the Internet Society's Global Internet Report for 2017 (see the Annex - Additional Resources)

- If my company's use of data was published in a news story tomorrow, would I worry about our reputation?

If the answer to either of these questions is 'yes', then the concerted application of the three principles the Internet Society sets out below will help data handlers understand and remedy the problem.

Guiding Principles

The Internet Society offers the following guiding principles to help all data-handlers – in public and private sectors and civil society – to fulfil not just the letter of the law, but its spirit and broader intent.

1 Transparency

User consent should not be used to obscure or excuse poor practice. If what you are doing with data would come as an unwelcome surprise to your customers or users, you should probably not be doing it. At the very least, you should be clear about what you are doing.

This means:

- Transparent, clearly and simply presented policies and information, and easy-to-access user controls, with privacy-respecting options as the default;
- Demonstrations that the organization is doing what it claims, and how safeguards are put into practice;
- Joining or initiating credible certification schemes for ethical data handling.

You should also be able to explain *why* you are doing what you do. Looking at the totality of the product or service you offer, you should be able to justify each decision made about data and how it is collected and used, and to show what ethical factors were taken into account in the decision-making process.

2 Fairness

Applying the principle of fairness means considering the data-impact of the product or services on users and stakeholders and the possible effects of failure or misuse, so that the result is a fair balance between everyone's interests.

For example, suppose a platform makes it possible for third parties to access users' messages. Users might have consented to their own messages being accessed, but messages go between two people. Has the other person given consent? Fairness to the other person might mean the platform should restrict what the third party can see.

Another way to think of fairness might be in terms of risks and costs, and benefits and revenues. If, for example, a public health scheme to share patient data with third parties means patients face risks and costs – e.g. expensive or denied health insurance in the future or increased exposure to the risk of a data breach – while the benefits and revenues of the scheme mostly go to the health providers and third parties, then fairness is at issue.

The principle of fairness builds on the principle of transparency because some of the implications for fairness may not be discovered if everyone does not understand what is happening. Fairness means extending the cost benefit analysis to the interests of everyone affected.

This means:

- Not using personal data for unfair discrimination, especially sensitive characteristics such as race, disability, sexual orientation, religion or political beliefs. (Note: even 'anonymized' data can include sensitive and identifying elements, and may be easier to 'de-anonymize' than you think.);
- Respecting the context in which data is collected and not using the data out of context, or in ways the person would not expect or consent to;
- Ensuring the data you hold about people is correct, and that it is collected, processed and, if necessary, shared on fair terms that they can reasonably understand.

3 Respect

Respect means addressing the wishes, interests and expectations of people affected by your use of data, and treating them as a person rather than as a means to an end. Respect for the individual is interpreted differently in different cultures, but it can form a common basis for ensuring that people are at the heart of decisions about data.

Treating data with respect means acting as the custodian or steward of other people's data, and protecting it on their behalf. This means elevating their interests in the collection, use and sharing of data.

Respect may mean:

- Excluding some third parties – such as advertisers or data-brokers - from the business model, or making it clear to people when what they think of as private interactions on social media platforms, for example, are observed and used by others;

- Showing consideration for users' limited time and attention, and not taking advantage of it to slip a long, unfavourable set of terms and conditions past them;
- Conducting due diligence on your use of data throughout its lifecycle, remaining accountable for it and ensuring people do not face worse terms and conditions as the result of the merging of services or companies;
- Promoting internal education and training in value-based design, continuous improvement processes, and the application of quality management disciplines to ethical data handling;
- Building the operational culture on a foundation of these principles, to ensure that people handling data apply ethical data handling practices to its use.

Recommendations

Recommendations to policy makers

- Strengthen the incentives for better practice:
    - Include responsible data-handling criteria in government procurements: require suppliers/partners to show how they put transparency, fairness and respect into practice in their policies, procedures, processes and products;
    - Provide a framework for certification schemes;
    - Stimulate the market for audit, and ensure penalties can be applied for bad practice;
    - Allow good practice to play a role in determining terms of insurance.

- Use the full range of applicable policy, legal and regulatory options, including:
    - Current and strengthened privacy and data protection laws;
    - Consumer protection and competition laws;
    - Programmes for education and awareness-raising;
    - Removing barriers to effective enforcement;
    - Increasing accountability through a "polluter pays" principle, so that the costs of bad practice are borne by the originator rather than the individual.

Recommendations for data handlers (across the public/private sectors and civil society)

- Be custodians of data, on the individual's behalf and in their interests.

- Adopt a principle of "no surprises"[3]:
    - Provide clear and relevant information to users, with simple controls and minimal collection by default;
    - Be transparent about what data you collect, and how you use and share it;

- Do not use personal data out of context, or for purposes the individual would not expect or to which they have not consented;
    - Do not use "consent" to excuse bad practice.

- Make ethical considerations explicit in your development process, so that you can show why you made the design and implementation decisions you did.
    - Consider how the costs, benefits, risks and impacts of your product or service are spread across all stakeholders, including non-user stakeholders: are you giving rise to risk and cost that will be borne by others?

- Respect the individual's interests, time and attention.

- Build an operational culture of transparency, fairness and respect:
    - In your business/operational plan, include the enabling and sustaining measures to maintain and strengthen that culture.

[3] This reflects an issue identified in the Internet Society's 2015 Global Internet Report (see the Annex - Additional Resources)

Annex - Additional Resources

The ethical themes of responsible data handling explored in this brief are not new to the Internet Society's advocacy efforts. They reflect concerns that have been addressed, for instance, in the Global Internet Reports (GIRs) the Internet Society has produced annually since 2014. Notably, from being a single recommendation in the 2014 GIR, ethical considerations grow steadily and are a pervasive theme of the 2016 and 2017 reports.

2014 GIR - Open and Sustainable Internet[4]

Recommendation #2: "There is a real need for the global community to come together and agree on strong ethical principles for Internet data-handling."

2015 GIR - The Mobile Internet[5]

Challenge: "Many of us also are surprised when confronted with the resulting data on our location and movements that is stored and shared among a variety of companies. The same is true for other types of personal and possibly sensitive data available through our smart devices."

Recommendation: Give users the means to understand and express privacy preferences simply and conveniently. [Note that this imposes an ethical obligation on the data controller]

2016 GIR - Data Breaches[6]

Issues: Negative externalities in the economics of personal data mean that data controllers lack the incentive to invest in data security - and when they do invest, they lack the means to signal that in ways that influence users' choices in the market.

Impact: Data breaches impact trust. There is no economic reason for organisations to account for this, *but it is an impact society cannot neglect.*

[4] https://www.internetsociety.org/globalinternetreport/2014/

[5] https://www.internetsociety.org/globalinternetreport/2015/assets/download/IS_web.pdf

[6] https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf

Recommendations: [The 2016 GIR's recommendations anticipate the ethical themes of this brief.]

- Put users at the centre of solutions [Fairness and Respect]
- Increase transparency about data breaches [Transparency]
- Adopt best practice for data security
- Ensure accountability, through liability and remediation [Accountability]
- Encourage good practice by stimulating a market for independent assessment.

2017 GIR - Paths to our Digital Future[7]

Themes:

- "Ethics will grow in importance as technical innovation accelerates and impacts people's lives".
- The global Internet and society reflect each other; it's vital to put people first.
- Ethical considerations, based on public debate about standards and norms, should be embedded in the design and development of new technologies.
- Human rights are the foundation;
- Users' interests must come first with respect to their personal data;
- Government action and competition policy must come together to make the Internet *economy* work for everyone.

Recommendations:

- Close the liability loop, so that the costs of bad behaviour are borne by those responsible.
- Make it possible for insurance to reward virtuous behaviour.
- Ensure that roles, responsibilities and liabilities in the digital ecosystem are clear. Acknowledge the interrelation of social and online behavioural norms: multi-stakeholder engagement, and increased responsibilities for online platforms, are an important next step.

[7] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf