Empowering digital citizens

Making humane markets work in the digital age

April 2023
A Global Initiative for Digital Empowerment of over 70 international specialists including policy experts, researchers, Internet technical experts, business people, online and security specialists and others.

Dedicated to the reformation of rules for the global digital economy.

Prioritize the broad interests of all people, rather than just businesses and governments, which are too often the primary benefactors of today’s digital economy.

Supported by The New Institute and the Global Solutions Initiative.
A majority in the global survey of 20 countries agree that new government policies are required to improve internet trust

<table>
<thead>
<tr>
<th>Policy</th>
<th>Greatly Improve</th>
<th>Somewhat Improve</th>
<th>Total Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies to protect Internet user privacy</td>
<td>27</td>
<td>38</td>
<td>65</td>
</tr>
<tr>
<td>Policies to protect your data</td>
<td>28</td>
<td>37</td>
<td>65</td>
</tr>
<tr>
<td>Policies to provide cybersecurity to Internet users</td>
<td>25</td>
<td>38</td>
<td>63</td>
</tr>
<tr>
<td>Policies to set standards for how Internet companies make use of user data</td>
<td>24</td>
<td>38</td>
<td>62</td>
</tr>
<tr>
<td>Policies to set standards for how Internet companies collect user data</td>
<td>24</td>
<td>38</td>
<td>62</td>
</tr>
<tr>
<td>Policies to allow you to control your data</td>
<td>24</td>
<td>38</td>
<td>62</td>
</tr>
<tr>
<td>Policies to set standards for Internet service provider activities</td>
<td>19</td>
<td>40</td>
<td>59</td>
</tr>
<tr>
<td>Policies to protect your country from other countries in cyberspace</td>
<td>23</td>
<td>36</td>
<td>59</td>
</tr>
<tr>
<td>Policies to control the sharing of online content</td>
<td>17</td>
<td>36</td>
<td>53</td>
</tr>
<tr>
<td>Policies to set product standards for Internet of Things devices</td>
<td>16</td>
<td>37</td>
<td>53</td>
</tr>
<tr>
<td>Policies to control the production of online content</td>
<td>16</td>
<td>36</td>
<td>52</td>
</tr>
<tr>
<td>Policies to regulate the development of AI</td>
<td>14</td>
<td>34</td>
<td>48</td>
</tr>
<tr>
<td>Policies to regulate the use of AI</td>
<td>15</td>
<td>33</td>
<td>48</td>
</tr>
<tr>
<td>Policies to regulate the purchase and sale of cryptocurrencies</td>
<td>15</td>
<td>29</td>
<td>44</td>
</tr>
<tr>
<td>Policies to regulate the use of cryptocurrencies</td>
<td>14</td>
<td>30</td>
<td>44</td>
</tr>
</tbody>
</table>

This survey was conducted in 2021-22 by Ipsos for Fen Osler Hampson, Carleton University, and Visiting Fellow, The New Institute.
Developing countries citizens have the highest level of concern about online privacy.

<table>
<thead>
<tr>
<th>Region</th>
<th>Very Concerned</th>
<th>Somewhat Concerned</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>32%</td>
<td>47%</td>
<td>79%</td>
</tr>
<tr>
<td>APAC</td>
<td>32%</td>
<td>51%</td>
<td>82%</td>
</tr>
<tr>
<td>Latin America (LATAM)</td>
<td>40%</td>
<td>42%</td>
<td>82%</td>
</tr>
<tr>
<td>North America</td>
<td>28%</td>
<td>53%</td>
<td>82%</td>
</tr>
<tr>
<td>Middle East/Africa</td>
<td>43%</td>
<td>38%</td>
<td>81%</td>
</tr>
<tr>
<td>Europe</td>
<td>22%</td>
<td>49%</td>
<td>71%</td>
</tr>
</tbody>
</table>

Base: Total respondents (n= 14519) ; 2019(n=23,854)
Q1.1 How concerned are you about your online privacy?
Problems generated by present regime

- Inadequate protection of privacy
- Inadequate cybersecurity
- Psychological damage – addiction, self-harm, depression, hate speech, attention capture, concentration damage
- Social damage – social exclusion, victimization, bullying, peer pressure
- Misinformation and eroded appreciation of truth
- Undermining market economies
- Undermining social cohesion
- Exploitation of psychological weaknesses
- Inequities – asymmetries of information and power, inadequate opportunities to shape terms of network participation
- Social, economic and political manipulation
- Social damage – social exclusion, victimization, bullying, peer pressure
Source of the problems

Third-party-funded digital barter, leading to a misalignment of interests between the digital consumers and the third-party financiers
The digital trade model

3. PROBLEMS WITH PRESENT DATA GOVERNANCE REGIME

VISIBLE TRADE

- Traditional revenue
  - Products
  - Revenue

INVISIBLE TRADE – DIGITAL BARTER

- Additional revenue from personal information
- Additional revenue from behavioral modification

Payment, influence

Information

Digital service providers

Consumers

Other producers

Other influencers

Digital services, influence
Personal information
The digital trade model

3. PROBLEMS WITH PRESENT DATA GOVERNANCE REGIME

**The digital trade model**

**VISIBLE TRADE**
- Products
- Revenue

**INVISIBLE TRADE – DIGITAL BARTER**
- Additional revenue from personal information
- Additional revenue from behavioral modification

**Traditional revenue**
- Personal information
- Behavioral modification

**Digital services, Influence, Personal information**

**This operates as a market**
- Digital service providers
- Consumers

**This does not operate as a market**
- Other producers
- Other influencers

Payment, influence
Information
Current policy approach

Treat symptoms in isolation

- Competition laws
- Privacy policy
- Injunctions against hate speech
- Consumer rights guidelines
- Business practices laws
- Taxes on digital transactions
- Fines for digital fraud
- ...

Result

Policy makers engage in a never-ending battle against systematically inappropriate incentives
The way forward?

Give users control of their data, individually and collectively.

In a topological network, which knows no geographic boundaries, the best way to achieve sovereignty and more equitable digital economic power is to empower the data sovereignty of citizens.
Proposals 1: Ensure citizens’ control over their personal data and who has access to it.

- Personal Data, such as defined in the EU’s General Data Protection Regulation, should be maintained by citizens in a trusted repository and citizens should have the obligation to ensure that the data is authenticated by the state of legally accepted sources.

- The citizen controlled repository should be the sole initial legal source of this data for public and private transactions, unless specifically stated otherwise by law. The data accessed by an entity could carry a transaction-specific digital signature confirming that the data in the hands of the entity has been sourced correctly. Such data holdings will be open to audit.

- Citizens should have effective control mechanisms over who accesses data about them and should be able to negotiate the terms and conditions under which such data is processed, through easy-to-use technical tools and supporting institutions.

- Provide GAAP-like audit oversight to data aggregators/traffickers with regard to the protecting the data they hold to ensure that the source of Personal Data is only the required citizens’ trusted repository.
Proposals 2: Enable citizens to negotiate the terms under which their personal data is used

- Provide effective rights of association and representation for citizens to ensure that professionals skilled in the data markets can advise groups of citizens, and negotiate on their behalf, about what terms should apply to the use of their Personal Data.
Proposals 3: Protect vulnerable citizens by imposing fiduciary obligations on the use of inferred data

- Ensure that entities which infer information about an individual from data which the citizen does not create have to abide by the duty-of-care rule that commonly applies in the offline world (for instance, between doctors and patients) - the data can only be used in the “best interests” of the data subject.
Proposals 4: Establish effective and accountable Data Commons

• Create accountability and legal structures to support the establishment of 'data commons,' which will consist of citizen communities with common interests who can pool personal data for the public good (e.g., medical research). (The recent EU Data Governance Act illustrates such a legal structure.)

• Ensure that common cata are under the control of effective, trustworthy and competitive organisations that promote the benefits of data subjects and the broader society.

• Ensure that the data commons are permitted to use data only for specified purposes and that its use be transparent and accountable.
Proposed eco-system

**Citizens**
- Right of association

**Representatives**
- Engage citizens
- Explain aspects of value in data market
- Record citizens preferences
- Ensure collection and update of authenticated data from citizen
- Pass data and preferences to data registry
- Establish citizen’s value account

**Data registries**
- Store data securely
- Encode data with preferences
- Inform representative and/or citizens of data request
- Share data with requestor according to citizens’ approval and preferences
- Encapsulate data with hash/digital signature specific to each requesting entity

**Look-up and data transfer system**
- Request data, as required, when establishing an account or first use of Official type data
- Negotiate types of conditions for privy data with representatives
- Accept/reject preferences put in citizen’s profile
- Keep digital signature with data for future auditing
- Make value transfer to Citizens’ accounts
Multiple technologies exist to support proposed data flow

Existing examples

- High Speed databases/resolution (e.g. DNS, PCCI)
- Hybrid block chain data storage (e.g. Seal)
- Personal ID wallets interacting with Data Exchanges (e.g. European eID)
- Personal Info Vaults interacting with Data Exchanges (e.g. Flemish Data Vaults)
- Tim Berners Lee’s social linked data initiative (e.g. Solid and Inrupt)
- Self Sovereign Identity movement (e.g. Sovrin or Germany’s IDunion consortium)

Result

Policy makers do not need to pick a technology to implement these policies. They can either encourage an industry standard development or promote technological competition (providing there is full interoperability)
Thank you

paul.twomey@thegide.org