Data Rights Protocol

A technical standard for exchanging data rights requests, incubated at Consumer Reports Innovation Lab

Ryan Rix - DRP Technical Lead
When Consumers Tried to Opt Themselves Out

- About 46% of the time, consumers were left waiting or unsure about the status of their DNS request.
- About 52% of the time, the tester was “somewhat dissatisfied” or “very dissatisfied” with the opt-out processes.
- For 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a “Do Not Sell” link on 12.6% of sites.
- add[ed] to a marketing list
- required to set up an account to opt out

California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?

MAUREEN MAHONEY
OCTOBER 1, 2020

Are Consumers’ Digital Rights Protected?
A model for improving access to data rights
• 3 of 21 companies (14%) did not provide confirmation that all of the opt outs had been processed.
• 1 of 21 companies (5%) requested non-standard information that we had not collected from consumers.
• 12 of 21 companies (57%) ultimately confirmed that they stopped the sale of at least some data in response to all of the opt-out submissions.
When Consumer Reports Submitted DSAR Requests

- Verifying consumer identity was difficult and confusing
- Some data seemed fishy to consumers
- Some companies weren’t fully prepared to serve consumer data rights or work with Agents

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fulfilled</td>
<td>51</td>
</tr>
<tr>
<td>Denied</td>
<td>38</td>
</tr>
<tr>
<td>Not fulfilled</td>
<td>8</td>
</tr>
<tr>
<td>Unknown</td>
<td>111</td>
</tr>
<tr>
<td>Total</td>
<td>208</td>
</tr>
</tbody>
</table>

Findings from helping 104 consumers access their own data from companies

“Cyber Specialists” by Khahn Tran is licensed under CC BY 4.0
CR’s Permission Slip is Building Tools for Consumers

Introducing Permission Slip, the App to Take Back Control of your Data

- Consumer Reports decided to build an agent app
- Users see a stack of cards explaining companies’ data practices informed by Privacy Policies and results of prior requests
- Currently driven by back of house, largely un-automated process
- How do we scale up to build something more consumers can take advantage of?

✨ Automation ✨
The birth of the Data Rights Protocol

- Consumers want to exercise their data rights, how can we streamline this process?
- Lack of strong verified digital identity limits businesses’ ability to respond to data rights requests
- Lack of consistent interface to requesting and tracking data rights hampers consumers’ ability to exercise these rights
- Authorized Agents are an opportunity to solve both issues at once
- The DRP is an organization of Authorized Agents, Privacy Compliance Tooling providers, and businesses to standardize and streamline the interchange of data rights requests.
The goal is to deploy a holistic Data Rights System in three dimensions:

- Technical protocol
- Operating rules
- Participatory network
The goal is to deploy a holistic Data Rights System in three dimensions:

- Technical protocol
- Operating rules
- Participatory network

Technology
Legal
Business
Technically, DRP is...

An interoperable request schema and state tracking

- Consumer identity, request status, delivery dates and deadlines

Fairly boring technology

- HTTPS, JSON, libsodium signing

A Simple root of trust

- validating Agent identity
- discovering DRP businesses
Technically, DRP is...

An interoperable request schema and state tracking

- Consumer identity, request status, delivery dates and deadlines

**Fairly boring technology**

- HTTPS, JSON, libsodium signing

A Simple root of trust

- validating Agent identity
- discovering DRP businesses

**POST /v1/data-rights-request**

```
base64(<signature> {
  "meta": {
    "version": "0.9"
  },
  "regime": "ccpa",
  "exercise": "sale:opt-out",
  "name": "Jane Doe",
  "email": "jane.doe@example.com"
})
```
Technically, DRP is...

An interoperable request schema and state tracking

- Consumer identity, request status, delivery dates and deadlines

Fairly boring technology

- HTTPS, JSON, libsodium signing

A Simple root of trust

- validating Agent identity
- discovering DRP businesses
Lightweight self-governance of the bounded network of participating businesses

- **DRP common agreement**
  - Describe relationship between Privacy Infrastructure Providers and Covered Businesses
  - Define participation rules and acceptable behavior between Agents and Companies
  - Outline eligibility requirements

- **Transparent documentation of data handling practices**
  - Businesses have Privacy Policies
  - Agents also have Privacy Policies as well as documentation of identity verification processes
Lightweight self-governance of the bounded network of participating businesses

- Lightweight operational organization w/o large ongoing costs
  - One vote for each organization
- Implementation certification using open source test suite and reference implementation
- Github Pages for organizing and deploying service directory
  - Agents, Businesses, and PIPs “nominate” a technical contact to manage their entries in the directory
  - PIPs can be “delegated” control over multiple Business profiles in the same way businesses delegate their Privacy compliance services to the PIP
Data Rights Protocol is a bounded network of innovative businesses

- Consumer authorizes agent
- Agent helps consumer submit request
- Privacy compliance tech facilitates request
- Covered business processes request
DRP is not just Consumer Reports:
Let’s make data rights real.

- [https://datarightsprotocol.org](https://datarightsprotocol.org)
- datarightsprotocol@cr.consumer.org