Cookies are bad.

We should replace them.
Perhaps with draft-west-http-state-tokens?

MY HERO

A two-step plan!

1. Stop doing bad things.
2. Start doing good things: draft-west-http-state-tokens.

```
cmv2=true; HomepageMarket=de; mmapi.HMPG23_market=de; mmapi.HMPG23_lang=en;
CONSENTMGR=c1:1%7Cc2:1%7Cc3:1%7Cc4:1%7Cc5:0%7Cc6:0%7Cc7:0%7Cc8:0%7Cc9:0%7Cc10:0%7Cc11:0%7Cc12:0%7Cc13:0%7Cc14:0%7Cc
15:0%7Cts:1554220801803%7Cconsent:true; mmapi.MM_gdpr=%5Bnull%2C%221%22%2C%221%22%2C%221%22%5D;
_ga=GA1.2.1179103170.1554220806; _gid=GA1.2.543082437.1554220806;
xctg_trace={"choice":3,"data":"DE","ts":1554220805723,"uid":"vZhSQO80bcHX"}; xctg=cf45812c95abebc5d84c2c54de39b98d;
_gcl_au=1.1.1844762224.1554220806; et_uk=7ec5384edf8d44dcae0d80e49b29bc04; mmapi.FM-search=true;
TLTSID=798D15B6556010550C66A7BA4A0271D0; TLTUID=798D15B6556010550C66A7BA4A0271D0;
um_jst=B2CBE35D14EEC727773F899D74B45FFB3555FA3B47F2990A26E0AE3BFBF58B94; DWM_XSITECODE=LUFTLUFT; AKA_A2=A;
searchFlightHistory=%5B%7B%22airline%22%3A%22LH%22%2C%22cabin%22%3A%22E%22%2C%22nbAdt%22%3A1%2C%22nbChd%22%3A0%2C%2
2nbInf%22%3A0%2C%22tripType%22%3A%22R%22%2C%22departureDate%22%3A%2220190403%2C20190410%22%2C%22from%22%3A%22MUC%2C
AMS%22%2C%22to%22%3A%22AMS%2CMUC%22%7D%5D; WCXSID=23799398278851383332O3469927;
mmapi.store.p.0=%7B%22mmparams.d%22%3A%7B%7D%2C%22mmparams.p%22%3A%7B%22pd%22%3A%221585756848957%7C%5C%2229510616 4%
7CBgAAAApVAwDgiLXVehE%2BCwABEQABQpvpkAoBAGs442CEt9ZIaxZ%2FQYS31kgAAAAA%2F%2F%2F%2F%2F%2F%2F%2F%2F8ABkRpcmVjdAF6E
QEAAAAAAAAAAAAHFQAAu9QBAMkpAgADAAgDAQCyYBsTU3oRAP%2F%2F%2F%2F8BehF6Ef%2F%2FAQAAAQAAAAABZIsCABI5AwABu9QBAAEAAAAmAgEA
GiVzm3V6EQD%2F%2F%2F%2F%2FAXoRehH%2F%2FwEAAAEAAAAAAUOJAgBLNgMAAbvUAQABAAAAywUBAEjzg8v2ehEA%2F%2F%2F%2F%2FwF6EXoR%2F
%2F8BAAABAAAAAAHXkQIAakEDAAG71AEAAQAAAAAAAAAAAAUU%3D%5C%22%22%2C%22srv%22%3A%221585756848969%7C%5C%22fravwcgeu06%5C%
22%22%2C%22uat%22%3A%221585756852964%7C%7B%5C%22mmPageID%5C%22%3A%5C%22FFPP_DE_gb%5C%22%2C%5C%22Language%5C%22%3A%5
C%22en%5C%22%2C%5C%22BFT%5C%22%3A%5C%22CONTDOM%5C%22%2C%5C%22Passengers%5C%22%3A%5C%22%5C%22%2C%5C%22Children%5C%22
%3A%5C%22%5C%22%2C%5C%22Babies%5C%22%3A%5C%22%5C%22%2C%5C%22Search_Mode%5C%22%3A%5C%22%5C%22%2C%5C%22OandD%5C%22%3A
%5C%22%5C%22%2C%5C%22TimeTillDep%5C%22%3A%5C%22%5C%22%2C%5C%22Trip_length%5C%22%3A%5C%22%5C%22%2C%5C%22TimeSpend%5C
%22%3A%5C%2241-60%5C%22%2C%5C%22Class%5C%22%3A%5C%22%5C%22%2C%5C%22RoomCat%5C%22%3A%5C%22%5C%22%2C%5C%22Flight_Cat%
5C%22%3A%5C%22%5C%22%2C%5C%22HomepageMarket%5C%22%3A%5C%22de%5C%22%2C%5C%22CustomerStatus%5C%22%3A%5C%22notLoggedIn
%5C%22%7D%22%7D%7D; mmapi.store.s.0=%7B%22mmparams.d%22%3A%7B%7D%2C%22mmparams.p%22%3A%7B%7D%7D;
utag_main=v_id:0169dec749e0005b2baa7be9ae2804072002806a009dc$_sn:1$_se:4$_ss:0$_st:1554222653013$ses_id:15542207963
90%3Bexp-session$_pn:3%3Bexp-session$dc_visit:1$dc_event:4%3Bexp-session$dc_region:eu-central-1%3Bexp-session;
D_IID=1502EAB7-C8C0-3DA3-8086-F292CC8A02AA; D_UID=A6F9F671-3909-39BF-A2E0-246F89286660;
D_ZID=97C04D55-38D2-3EF8-A222-6DBC2AB493C3; D_ZUID=D2FB279A-1676-3D92-BB9F-53BFA3EE55AD;
D_HID=CFD80DE8-26ED-3A38-A36C-AB1DCA1F7530; D_SID=46.142.202.162:jxnXA8O4itb+VDUmT+uRzxJ37kTMaudNuOpbXpNRDko;
TLTHID=93C0395455601055 15B28F89F4E07D02
```

Cookies' default settings are bad for security.

HttpOnly	~6.8%
Secure	~5.5%
HttpOnly; Secure	~3.1%
SameSite=*; Secure	~0.06%
SameSite=*	~0.05%
HttpOnly; Secure; SameSite=*	~0.03%
SameSite=*; HttpOnly	~0.006%
__Secure-	~0.005%
__Host-	~0.01%

Cookies are inefficient.

Percentile	**Cookie Header Length (~bytes)**
5%	36
25%	145
50%	481
75%	879
95% *(The header you just saw)*	2805
99%	5483
99.5%	6521
99.9%	9269

Cookies' default settings are bad for privacy.

Plaintext delivery enables pervasive monitoring.

Third-party delivery enables not-quite-so-pervasive monitoring.

```
__Host-token: key=value;
              Secure;
              HttpOnly;
              SameSite=Lax;
              Path=/
              ~~Domain=whatever~~
```

Perhaps we could do something different:

```
Sec-HTTP-State: token=*erWLK...RirDLk*
```

Default behavior.

```
Sec-HTTP-State: token=*erWL...DLk*
```

- Browser-controlled value.
- No JavaScript access.
- Origin-bound.
- One token per origin.
- No plaintext delivery.
- Same-site delivery.
- 1 hour lifetime.

Configuration options?

```
Sec-HTTP-State-Options:
    delivery=same-origin,
    max-age=2630000,
    ...
```

Delivery Scope

```
delivery={
    same-origin,
    same-site,
    cross-site
}
```

Lifetime

```
max-age=3600
```

```
// On expiration:
let resetChannel = new BroadcastChannel('http-state-reset')).;
resetChannel.onmessage = e => { /* Do exciting cleanup here. */ };
```

Some control over the value?

```
value-prefix=*VFuf*
```

Proof of Provenance?

```
key=*uzpV...1KaC3UxbI*
```

```
Sec-HTTP-State: token=*token*, sig=*HMAC-SHA265(key, token+metadata)*
```

Feedback?

1. Skim the draft:
   draft-west-http-state-tokens
   (also with pretend pages!)

2. File issues on GitHub:
   mikewest/http-state-tokens

3. Yell at me on Twitter:
   @mikewest