Infotrust eXchange

Information Trust Exchange Governing Association
http://www.itega.org

Bold thoughts about a billion-dollar opportunity?

Wrapping up the Multistakeholder Privacy Initiative's first collaboration in Chicago[1]

(This report comprises a two-page executive summary and and expanded eight-page wrapup)

A. EXECUTIVE SUMMARY

A bold effort to put the news industry at the forefront of helping users gain more control over their privacy and digital identity – and build a fresh funding source for journalism governed by a nonprofit entity – emerged as a "moonshot" proposal at a meeting of stakeholders Sept. 26-28, 2018, in Chicago.

The idea emerged from three days of talks that included about 25 people, including news publishers and broadcasters, privacy advocates, technologists, academics and others. A special initiative of The Internet Society (ISOC), headed by a former U.S. Commerce Department deputy secretary, worked with two other groups to arrange the proceedings. A second meeting is planned for January, with some efforts started in the meantime.

The two organizations helping ISOC with its Multistakeholder Privacy Initiative are:

- The Local Media Consortium, a for-profit, non-equity S-corporation with 80 holding-company members operating 2,200 local media sites and drawing 168 million unique visitors reaching 65% of the internet audience.

- The Information Trust Exchange Governing Association, a 501(c)3 nonprofit public-benefit corporation seeking to improve the web by helping consumers manage their privacy, elevate the relevance and value of advertising and make possible a shared "fast pass for news."

The "moonshot" idea includes:

- Creating a nonprofit initiative supported by news publishers/broadcasters, advertisers, browser-software makers and foundations -- to improve and innovate in the way the web handles user personal information.
- Fostering a nonprofit platform – or "cocoon" -- for managing user data for advertising and other purposes.

[1] -- This summary was written by Bill Densmore, executive director of the Information Trust Exchange Governing Association based upon contemporaneous notes of proceedings interpreted to respect the Chatham House Rule.

- Give consumers the option to join the "cocoon" through their local news organization, and then negotiate terms under which their personal attributes and web browsing activity may be shared with other trustworthy publishers in the network.

The network login via trustworthy news organizations would form the basis for an advertising or direct payment network for news, governing by rules established by the non-profit governing organization. It would represent a culture shift to connect users with news organizations in an open, pro-privacy environment designed to:

- Enable a unified "login" across news organizations
- Incentivize the use of privacy tools
- Educate about privacy options and choices
- Certify or otherwise suggest limits on advertising technology based upon reputation and practices
- Certify or identify trustworthy web and mobile services

Beyond merely setting up a governance and public-education campaign, the Multistakeholder Privacy Initiative developed these concrete enabling steps:

- Work on a standard set of privacy rules and protocols that major news publishers and broadcasters could choose to embrace.
- Identify and stand up an operator of a nonprofit anonymized user-data exchange that would be in a "first-party" relationship with the public.
- Support moves by major web-browsing software makers, including Apple (Safari) and Mozilla (Firefox) to make it easier for the public to withhold consent to be "tracked" across the web, accepting the browser as a legitimate enforcement tool.
- Enable a review of scholarly research on consumer attitudes about privacy, with the possibility of fresh anthropological study if needed.

Testing of a prototype Global Consent Manager (GCM) application under development jointly by the University of Missouri and the University of Oklahoma. With support from the Donald W. Reynolds Journalism Institute. The GCM would become an optional "plug in" extension to browsers, allowing users to pre-set their privacy preferences and have them automatically recognized by websites judged trustworthy by them or by a certifier they trust. GCM means not having to deal with multiple pop ups asking for data-usage consent. The intent is to turn it from a publisher-managed process to getting consent and saying as a user, "I'm going to your site; I'm telling you what my consent is going to be; so listen to me in dealing with whatever pop-ups you want to show me."

END OF EXECUTIVE SUMMARY

B. CANDID CONVERSATIONS

In order to be able to speak candidly without representing their organization, participants in the Chicago talks agreed not to be quoted by name or affiliation. Among some emergent themes:

- Consumer privacy can be a real differentiator for publishers and that is a benefit for advertisers who are looking for quality placements. For publishers to start a relationship with their stakeholders over privacy, standards can be established by government regulation or by collective nonprofit governance action.

- Industry usability studies show consumers prefer that third-party tracking be turned off at the browser level because it improves website performance and causes fewer browser crashes and hang-ups. They also use the web more with "third-party cookie" tracking off. There's a need for "intelligent tracking protection" that enables consumer choices that recognize the need for publishers to continue - to make money through ethical advertising.

- The level of public confusion and lack of knowledge about how browsers and advertising-technology works means a key pathway to success is to just try things and see how the consumer responds. “You have to get to them as early as possible and just say, ‘How does this work for you,’ ” said one participant. Another participant said a starting point should be trying to understand consumer wants and needs, and stating test offerings in terms they understand well enough to thoughtfully reject or accept.

C. SINGLE-STATE LOGIN NETWORK?

Day 1 in Chicago included discussions of how publishers can benefit by creating a single-state login for the news category, a trust network for the open web. It was seen as needing to start with some agreement with consumers about what you're going to do on the network -- what is being “consented” across it. It could help news organizations to acquire new audiences, by getting direct consent from people to fairly share their data. A universal login has the advantage of sharing the “state” of the user – and perhaps sharing some user-opted-in-preferences and service-level information – without using cookies.

Said one participant after Chicago:

> *The signed-on state at scale will provide publishers with an avenue to first-party data without the need for a "cookie" or third-party tracking method. It will allow publishers a state congruent with Facebook (and others). That is, publishers will be able to track all activity as long as the logged-in state is maintained. There is a privacy issue related to this in the US (and other places) needing to be addressed. Behaving in a manner similar to Facebook is not ideal. A consumer-friendly "agreement" (aka, policy, TOS, promise, technology) needs to be developed and deployed clearly spelling out "tracking" and adhering to laws and the spirit of laws so consumers don't puke at the whole idea of a signed-on state across media.*

There may be as many as 150 million active news consumers in the U.S. alone who could be part of such a sharing network, it was asserted. The phased introduction of such a service might start with uniform privacy rules for sharing data and technology standards. Once achieved, there could be movement toward protocols for sharing data among web services – such as privacy-respecting “tags” on sites.

Said one participant: “Give users a way to say yes or no. If we are going to build a future data environment we can build either the “over sharer’s” dream or the privacy nerd’s dream. We are going to have to have a situation where a lot of the traffic to a typical website is logged in traffic, but another set where they are not logged in -- but those ad impressions are still valuable because of some aggregate demographic or interest data from the logged in users.”

There was recognition that without critical awareness and education to accompany privacy-centric rules, a data-sharing network would be suspect in the public’s mind. The data would have be “used for good” from the consumers’ point of view, otherwise the public will be driven to more and more “ad blocking” tools.

Said another participant: “We are going to create this network . . . [that] is going to be built on trust rather than deception. The more you can say, ‘Look this is what we are doing, we are local media companies, we need revenue, this is what we are doing.’ The more you can be really direct about it the easier it will be.”

Said a third participant: “We may have different degrees of action but it is about giving that control back to the consumer.”

D. WHAT CONCERNS THE PUBLIC NOW?

The discussions at one point turned to this: What is most controversial and worrisome to the public?

Some answered offered:

- Behavioral profiling and ad retargeting

- The “data append” – supplementing web-browsing activity with data-broker demographics
- Social widgets which enable opaque tracking across much of the web by a single company
- Sharing of hashed identifiers, not because it is necessarily evil, but because it is below radar
- Obnoxious ads and “click bait”
- Data breaches, revealing of personal behavior, sharing of location data

The privacy situation in the United States is in flux because, compared with Europe, there is not much dedicated privacy law and the only enforcement mechanism is Section 5 of the Federal Trade Commission Act concerning unfair and deceptive practices. There are differing views about what the EU’s General Data Protection Regulation (GDPR) means, how to comply and how strictly its provisions can – or will be – enforced, particularly given uncertainty about the “legitimate interest” language.

A participant said there are as many as 40 proposals in various stages of consideration in the U.S. Congress or administration with one or more bills likely to be filed before the end of 2018.

E. WHAT MIGHT BE REASONABLE DATA COLLECTION?

A reasonable approach publishers and broadcasters might take, it was suggested:

- Anonymous, contextual data collected without consent necessary
- Lean against asking for more
- If you need more, make a clear public case and ask permission
- Don’t bundle permission for basic data collection with consent for deeper, out-of-context collection.

> *“The idea we were chatting about is building a consumer based more educated and smarter about their privacy,” said one participant. “Advertisers are going to want to reach that community. They are frustrated, they are going to want to be part of it.”*

F. WHAT ABOUT DIRECT PAYMENTS?

There was some limited discussion about subscriptions, donations and payments.

One participant asked: Is it possible for one user who joins a universal-identity pool to have “all access” to content in exchange for sharing a lot of data? It was observed that there has been little testing of that approach, since news organizations to date have generally pursued “siloed” pay walls rather than content-access across multiple, independent websites.

NPR’s success with local affiliate memberships changes the model of buying a bundle of content for a fixed price – rather it is a “pay what you think it is worth” approach. The Public Broadcasting Service’s member TV stations sign up donor members who then receive privileged access to streaming video at the PBS national website.

Nothing like these approaches exists for commercial news organizations yet. But the data show that there is a lot of traffic between and among news websites – the same users grazing in many fields. That has two consequences. The first is that some types of news are available in many places, so a single undifferentiated news site has a competitive challenge trying to block viewers who won’t share money or data. The second consequence is that a network of news sites, each of which has a little bit of unique content, becomes a potentially a valuable service when consolidated under a single sign on and pricing bundle.

Said one participant: “You have to be able to light up the network. . . . . there is a lot of traffic going between newspaper web sites.”

G. AD ECOSYSTEM DEATH AT DATE CERTAIN?

More discussion focused on the way advertising works on the web today, and whether the forcing function of browser-software attention to user privacy and data collection will change it.

In the **current environment**, a technology arms race works to try and identify the attributes of users without their consent, then track those users to all kinds of websites – reputable and tacky – to show them an ad perceived as relevant. This is often termed a targeted "direct mail" approach, or "programmatic advertising." Said one participant: "Advertising that tracks individuals tends to have negative externalities -- price discrimination, identity theft, fraud. That happens to be a section in which there are a bunch of competing companies and a lot of those companies cannot afford the security and safety practices to handle the data responsibly."

In a **second approach** potentially preferred by quality, trusted news organizations, the opaque effort to identity and "tag" users is replaced by one in which users are sorted based on where they congregate – web or mobile services focused on location, affinity or topic – and ads are served based on that "context." This is seen as a "brand-building" approach, and it is theorized that brand advertisers may prefer it.

News publishers make money in the current environment via both methods, and the question that seemed to be on the minds of participants is this: How much revenue would publishers lose by declining to serve "programmatic ads" vs. how much they would gain by protecting their user's privacy so they can only be found by advertisers in high-value "contexts." An ad-blocking, privacy-using person -- a desirable segment for advertisers -- is a segment that brands cannot reach in the programmatic ecosystem. If news organizations were to stop accepting programmatic ads on a certain date , could there be some way to bridge the revenue gap until contextual advertising came up to speed?

> *"If left to their own devices advertisers will seek as much data as they can. But if you get the cult of the willing, there is a growing set of people who want a different ad experience. Tell advertisers: Do the other stuff if you want to, but there is this valuable new segment."*
>
> -- A participant

H. WHAT'S POSSIBLE NOW? POLICY OR ARCHITECTURE?

Discussion turned to consideration of what steps might be possible for news organizations and privacy experts and others working collaboratively. Developing a "privacy policy" is useful, but cannot be divorced from the reality of what technology and business relationships can implement. Thus in some respects system architecture and business goals decisions come before privacy policy. "We can't separate the privacy discussion from the business-model discussion," observed one participant. A key consideration mentioned – balancing the need to support local journalism against the need to respect and enable user privacy choices. Said one participant: "If we took advertising out of the equation what are some of the other options -- innovative ways to support strong news ecosystems at the local level?"

> *"I don't see any of this happening without partnerships among publishers, browser makers and advertisers."*
>
> -- A participant

Some additional considerations emerged:

- Consider a privacy-safe badge or tagging program and protocols.
- Think about user credential portability – a shared-subscription model and data pool – with *real* enforcement mechanisms – such as a standards and certification process.
- For a news organization with a corporate culture of high integrity at the board level, active participation in a common vision that informs practice and outcomes, rather than just listing ideas and lists, was seen as desirable.
- Vendors offering solutions need to take legal responsibility for their impact.
- Pursue exploration of "enhancing the user relationship." Being up front and transparent is crucial for not just pay walls, but newsletters, subscriptions, enhanced

and shared content and/or quality advertising. Nuances are needed between subscribers and “fly-bys.”

- Better, more credible user relationships were seen as appealing to advertisers. A news-industry baseline of user-relationship quality would be desirable.
- Publishers, browser-software makers and advertisers need to be consulted and collaborating in some fashion.
- Move away from legacy business models that “bring people to a central location.” Google AdSense “monetizes” people in a million locations, for example. Try a content syndication approach.
- Develop a standard schema for how user data is maintained and transferred with permission. Use a nonprofit data-exchange model – a shared Data Management Platform (DMP).
- Stop trying to piece together fractured-ownership companies with “Scotch tape."
- Return to and elevate the proposition that the relationship with a user is an important value
- Browsers are generic software. Differentiating in support of publishers is an option.

I. MOVING THE GOAL POST?

The Multistakeholder Privacy Initiative leadership approached its first convening in Chicago with the idea that an initial step might be to develop a model privacy policy document and framework that could be adopted by many quality news organizations. But the evolving discussion seemed to move the goalpost -- calling for something broader – a reassessment and rebuilding of the trust relationship among publishers, broadcasters and their stakeholders.

What might provide enhanced trust? It was to that question the group turned by asking these three questions:

- What practices *not engaged in today* would provide for an enhanced trust relationship?
- What current practices are *barriers* to rebuilding trust?
- How might stakeholders sign up to be *accountable* for what approaches are taken?

Some suggestions for answering those questions included:

- Flesh out whether anyone has concrete technology or proposals yet for respectfully aggregating data among media companies.
- Identify practices and policies that would need to be in place.
- Develop flexibility between “privacy maximalist" and “revenue-centricity” for publishers.
- Figure out a brand identity for the efforts
- Communicate more clearly to site/service visitors on arrival what their data sharing and privacy options consist of.

J. HOW IT MIGHT WORK

The Chicago group began to form thoughts about how a service might work.

A missing piece for publishers presently is the ability to do user data collection (permissioned demographics and interests graphing) that is “obviously different from the bad stuff,” said one participant. “Otherwise it is seen and blocked by some browser software as just another tracker.” Right now, observed one participant, browser makers don't have answers to important questions that could help legitimate publishers and privacy-conscious users alike.

Another participant said the group seemed to be talking about deploying the technology in a partnership with a browser maker, where users come in and are authenticated and are pinged only by those advertisers – or by ad technology companies -- that are *approved*, *sanctioned* or *audited* to operate respectfully within a system that has privacy values built in. The advertisers can ping the permissioned, anonymized user data as they go.

Another participant said they envisioned users having a universal login that is "pseudo anonymized" and issued by one of many participating local media organizations, but recognized by hundreds of others within the network. The login could be supported by the browser, or by "wallet" technology on a user's device.

While browser makers would block cookie-based tracking among independent websites, a non-cookie based approach from a common domain – a shared coordinating server – might be viewed as permissioned and acceptable to the browser – an account that works across many pay walls, and user-data collection that conforms to network-privacy promises and standards.

While fielding such a system seemed like a "moonshot" idea, several participants said they viewed the challenge not as technical but as a matter of creating an environment in which publishers want to join a marketplace with common data and privacy standards, and protocols, but competition in pricing and services.

The other challenge expressed was this: Quality publishers receive meaningful amounts of revenue from programmatic networks that place ads on their digital channelswithout any sales effort by the publisher or broadcaster. While the CPM rates are low, it is seen as "found" revenue. But the networks also scrape up or derive behavioral data about the news organization's users, match it with other sources, and then serveads to those users at less-reputable websites. Publishers know this is happening but are loath to stop the revenue-flow from that business without a clear path to a replacement.

> *"We are talking about deploying the technology in a partnership with a browser maker, where users come in and are authenticated and are pinged by advertisers that are approved to be within a system that has privacy values built in. The advertisers can ping the permissioned, anonymized user data as they go."*
>
> -- Paraphrased participant

K. STOP THIRD-PARTY COOKIES FREEDOM DAY?

One participant suggested that, much as the GDPR enforcement took effect on a specific day, could an entity like ITEGA propose an "end to TP tracking" date that publishers could endorse and respect? Would that create lift for the development of alternatives?

Methods for detecting ad fraud were discussed in general. Other participants suggested that news sites could "turn off" such programmatic advertising placements for a set period of hours, and then audit with advertisers whether they appear to be fraudulently billed for bogus ad views during such an un-announced period. Would the results be of public interest?

L. PRIVACY PUBLIC EDUCATION

Discussion also revolved around the opportunity for news organizations to educate the public about privacy issues and offer help with managing personal data and identity. Could a public-benefit organization create a certification that could be applied by publishers and broadcasters who are part of such efforts to respect network privacy standards in their business?

A one-year "moonshot" process suggested to the group included:

- Single sign on log-in state operational
- No third-party tracking content networks allowed
- Commenting widgets removed

- Consumer education at a clear-and-simple level
- An easy-to-use presentation of how data is being used in real time
- A non-profit entity to foster deployment and partnership with a browser maker.

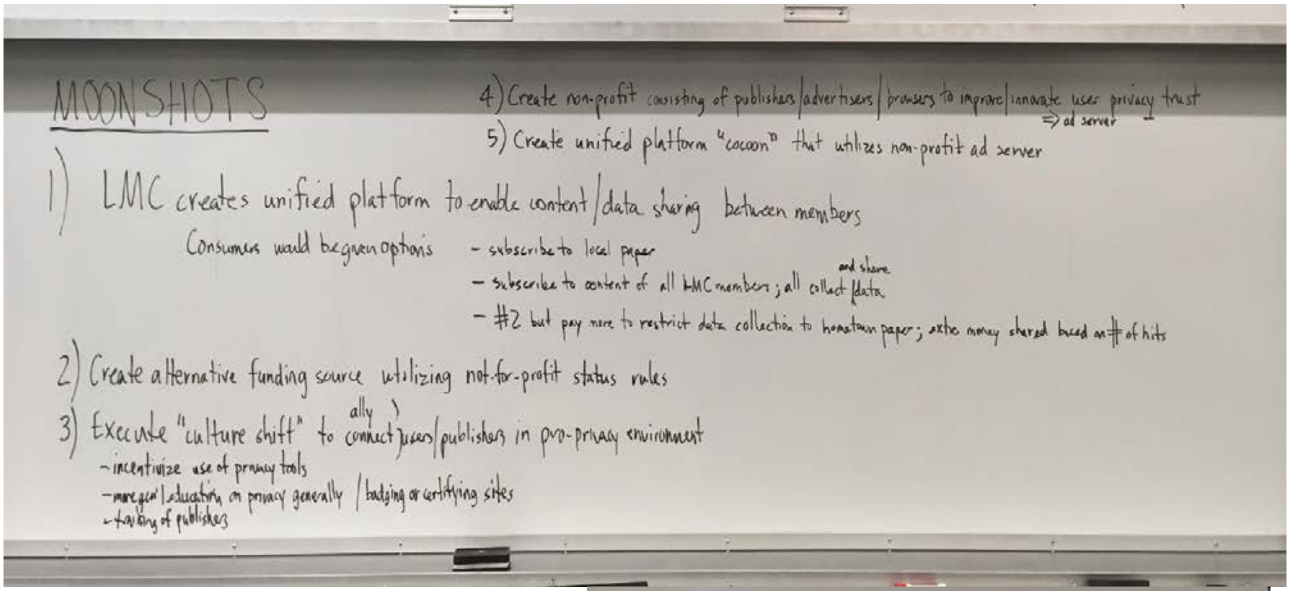
Here was one participant's idea of how to implement:

> *Create a single login user account with an encrypted wrapper that encodes the user permissions by default -- users can change those permissions when they want -- and which travels with the individual to various websites in the system; to ping the data based on information users have given. The participating member advertiser, network or publisher can use the data in real time but not store any data. The mission is to improve and innovate around user privacy and trust.*

One participant added: "The whole core problem here is it all starts at the ad server -- that's where it all begins. But the problem with not having it in a nonprofit is somebody is going to want to monetize it eventually." Another said it was an intention to create a "Netflix for news in which the identity of the user is protected."

M. FRAUD A MAJOR PIECE OF THE $100 BILLION PIE

Digital advertising is worth $100 billion a year globally, one participant estimated. Some $20 billion of that is projected to be fraudulently billed or represents advertising being seen in places advertisers don't want it seen. Any credible effort to cut down on fraudulent billing or ineffective ad placement could justify an expending of "big money," this participant said.



MOONSHOTS

4) Create non-profit consisting of publishers/advertisers/browsers to improve/innovate user privacy trust ⇒ ad server

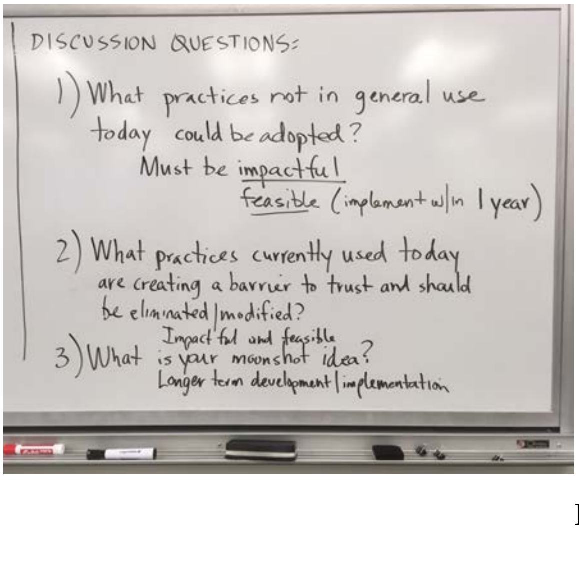
5) Create unified platform "cocoon" that utilizes non-profit ad server

1) LMC creates unified platform to enable content/data sharing between members

Consumers would be given options
- subscribe to local paper
- subscribe to content of all LMC members; all collect and share data
- #2 but pay more to restrict data collection to hometown paper; extra money shared based on # of hits

2) Create alternative funding source utilizing not-for-profit status rules

3) Execute "culture shift" to connect ally users/publishers in pro-privacy environment
- incentivize use of privacy tools
- more gen'l education on privacy generally / badging or certifying sites
- ranking of publishers

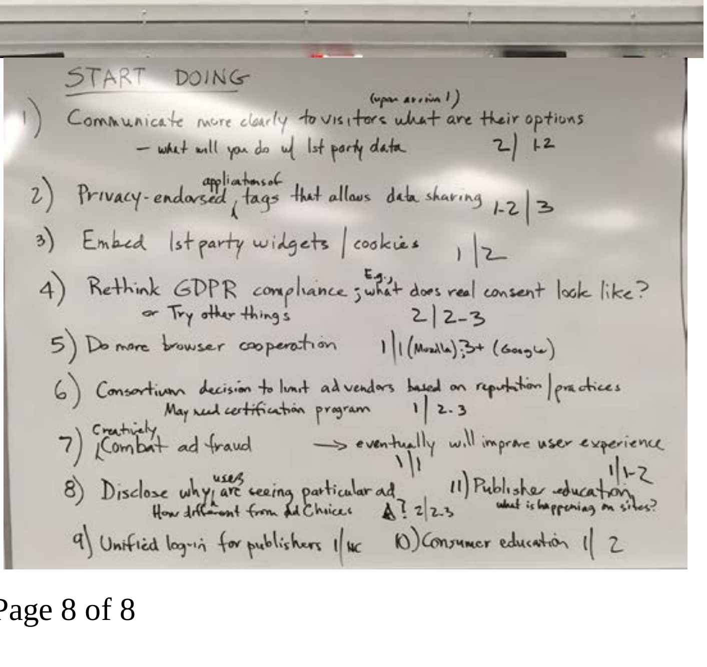


DISCUSSION QUESTIONS:

1) What practices not in general use today could be adopted?
Must be impactful
feasible (implement w/in 1 year)

2) What practices currently used today are creating a barrier to trust and should be eliminated/modified?

3) What is your moonshot idea? Impactful and feasible
Longer term development/implementation



START DOING

1) Communicate more clearly to visitors what are their options (upon arrival)
- what will you do w/ 1st party data 2| 1-2

2) Privacy-endorsed applications of tags that allows data sharing 1-2|3

3) Embed 1st party widgets / cookies 1|2

4) Rethink GDPR compliance; E.g., what does real consent look like?
or Try other things 2|2-3

5) Do more browser cooperation 1|1 (Mozilla); 3+ (Google)

6) Consortium decision to limit ad vendors based on reputation/practices
May need certification program 1| 2.3

7) Creatively Combat ad fraud → eventually will improve user experience 1|1

8) Disclose why users are seeing particular ad
How different from Ad Choices A? 2|2.3

9) Unified log-in for publishers 1|NC

10) Consumer education 1| 2

11) Publisher education 1|1-2
what is happening on sites?