DONALD W. REYNOLDS JOURNALISM INSTITUTE
Missouri School of Journalism University of Missouri

May 5, 2015
"Stalking horse" BUSINESS-MODEL EXERCISE
FOR RJI - OHARE ROUNDTABLE ON THE
INFORMATION TRUST EXCHANGE

Web link:
https://docs.google.com/document/d/1atq67XO449UWVdeyO2yRQw6eeWzU69DLF1VOtZ8rtok/pub
This is available for editing at:
https://docs.google.com/document/d/1atq67XO449UWVdeyO2yRQw6eeWzU69DLF1VOtZ8rtok/edit

PART ONE

ACTION CALL

Mass-market advertising is not sustaining journalism. Public engagement with the news is more and more happening on digital platforms that support sharing and comment on the news but do not do enough to underwrite its creation. News organizations are losing touch with their readers. RJI believes it can help with a solution. We want to help the industry, technologists, foundations and citizens to create a new, public-benefit platform for trustworthy sharing of valuable news and information, while helping the public manage privacy and identity. The Reynolds Journalism Institute has convened this meeting seeking guidance on whether it should proceed with an initiative with the working title – the Information Trust Exchange.

- Could a non-profit collaboration to share technology, users and content help set standards for convenient web/mobile information sale?
- Could it provide the public with more trustworthy information choices, and better privacy control?
- Is organizing such an effort feasible now?
- Should a steering committee be formed to establish a public-benefit collaboration for fostering identity, privacy and information commerce?
    - On what issues might a steering committee focus: Governance, membership, structure, security, content, commerce, privacy, identity, payments, other? (see: http://newshare.com/ite/steering-subgroups.pdf
    - What are the major deliverables for its work?
    - What is a realistic timetable for the work?
- If not a privacy-identity-commerce collaborative, then what?

"Stalking horse" BUSINESS-MODEL EXERCISE
FOR RJI - OHARE ROUNDTABLE ON THE
INFORMATION TRUST EXCHANGE

PART TWO

PROPOSED OBJECTIVES

- Provide the public convenient access to trustworthy, valuable customized content packages and services without multiple accounts and logins
- Provide one or more new business models for publishers that "level the playing field" vs. tech platforms like Google and Facebook
- Enable a range of privacy/identity trust alternatives for the public:
  - ☐ Offering an alternative between government regulation and investor-owned platform monopoly for online identity
  - ☐ Reducing by market force the proliferation of opaque, proprietary, unaccountable cookie-based tracking

BUSINESS-MODEL QUESTIONS

If we can reach rough consensus on the answers to the questions below, then out of that will come an ITE business model that stands a reasonable chance of gaining the necessary support of publishers and users—**and that is what RJI needs to move to the next step**.

FIVE PROBLEMS, FIVE DESPARATE SOLUTIONS FOR THE NEWSPAPER INDUSTRY?

(source: http://newshare.com/ohare/dire-straits-winter-wurzer.pdf

PROBLEMS

1. Lack of scale - no single newspaper company, no single newspaper, can compete on its own
2. Lack of money - fear of risk led to a policy of managing decline and low investment
3. Low competitive value - news is a commodity, local is a weak differentiator
4. No digital culture - products reflect low digital sensibility and are failing in the marketplace
5. Diminishing leverage – transaction throw-weight is declining every day

SOLUTIONS

1. Need a single voice and platform
2. Must be willing to put current traffic at risk
3. Must hire different people to build new digital products unencumbered by parent newspaper company interest
4. Must build shareable databases of local-registered users for our own product development, marketing and ad sales use
5. Must put in place our own sales force

PART THREE

STRATEGIC QUESTIONS

- Can a royalty-pool model be well adapted to news and other content (vs. song plays) when the perceived value of objects varies widely (MST vs. magazine vs. news, long vs. short, investigative vs. spot news)?

- Must a service support both bundled subscription, and per-item access to content?

- To gain marketer/advertiser participation, must the model include a mechanisms for monetizing personal data? If so, will users have control over the process? Must freemium be an option?

OPERATIONAL / TACTICAL QUESTIONS

- NETWORK SUBSCRIPTIONS -- Should the service allow publishers to be paid for providing digital content across an ITE network without having to have one-off relationship with each reader/user?

- DYNAMIC SERVICING -- Would publishers want to be able to have real-time personal, demographic or interest attributes of a user/reader at the time the user makes an online/mobile request for information, so they can respond with targeted, customized advertisements or messages or services?

- POOL PRICING -- Will publishers participate broadly in a system which does not allow them individually to control the value assigned to their content or services other than contractually on an aggregate basis as part of a system-wide royalty pool? (see: "Spotify" model)

- WHOLESALE-RETAIL PRICING – Will publishers appreciate and use a method for allowing them to establish the price they wish to receive (and be assured of payment) for a discrete digital object (or bundle), and be able to vary that price dynamically in real time based upon the attributes of the user requesting the object? (Amazon books model)

- ONE BILL/ACCOUNT – Should the service enable a user/reader to have one bill/one account/single sign-on access to information from (virtually) anywhere, by subscription or by click/action?

- UNIVERSAL TRACKING – In order to gain the participation of publishers and advertisers, is it necessary that the system enable a user's activity to be tracked across the ITE network and that activity aggregated – only -- to the user's home-base service provider for billing and analysis – all with permission of the user?

- CONTENT PACKAGING – In order to gain the participation of end users, is it necessary that the system permit custom assembly by the user of information services from a variety of topical and geographic-oriented sources into a personalized subscription package?

- FREEMIUM vs. FREE – In order to gain participant of both privacy advocates and the advertising industry, is it necessary that the system allow the public user to chose among a range of options from (1) no-advertising and no disclosure or use of their tracked activity in a subscription-based approach to (2) receipt of highly customized commercial messages and the wide, background marketing of their information preferences in a rewards-based approach?

- SUBSCRIPTION OR PER-CLICK – In order to satisfy the requirements of a plurality of publishers and service providers, does the service need to be able to offer end users both sale or receipt of digital items within a pre-paid subscription package as well being able to dynamically query the user if they want to purchase a particular resource on a one-time, one-item basis?

THESE LAST TWO QUESTIONS SHOULD BE CONSIDERED IN PARALLEL:

- PROFILE DATA FOR PUBLISHER – Will publishers be content to sell information resources to anonymized incoming casual or "drive-by" users (a la "newsstand customers") at a reasonable price they establish, or will they insist upon knowing detailed information about users other than their own users?

- PROFILE DATA FROM USER OWNER – Will ITE service providers who establish accounts and manage the persona and privacy of their users be willing to provide detailed demographic and interest information about those users to third-party publishers as a condition of those publishers being willing to provide services to someone else's users?

---

end of strategy / tactical questions

PART FOUR

A "stalking-horse" system description

May be read in conjunction with:
http://newshare.com/ohare/ite-summary-description.pdf

If the participant answers most of the business-model questions, above, with a "yes", then a reading of the rest of this document provides an operational approach.

A. System attributes
B. Visa/telco analogy
C. Some specific system elements
D. Two stakeholder groups

A. STALKING HORSE SYSTEM ATTRIBUTES

1) System tracks all clicks (that involve value exchange) in background, aggregating them, settling aggregated value exchange.

2) Each user service provider gets clickstream data about that user which it can use subject to TOS with the end user auditable and enforceable by the ITE as a condition of system membership.

3) Publishers (content providers) do NOT get identifiable information about any user (at least not from this system); they just get assurance that the person is authorized to view the resource requested and that, if money is involved, the money is going to be handled and they will get or give what they expect.

4) This does not stop publishers from setting their own cookies or doing other things to identify users, unless or until the Information Trust Exchange prohibits such behavior as a condition of membership.

B. ANALOGOUS TO VISA/MC OR PHONE COMPANIES?

What is proposed is similar in some respects to the Visa/MC model, but in one key way it is more like the way the phone companies settle their calling traffic -- they settle aggregated debits/credits among each other based on numbers of calls exchanged -- but their consumer customers may be paying for minutes in bulk. The system tracks every call because that is necessary even to provide unlimited calling packages to the public. This system as described permits a plurality of subscription packages with pricing as in a free market for digital information -- set by the service provider who holds the end-user's account, and also set by the publisher who wants pricing control over their content.

Where those two come together -- content sold at wholesale and subscriptions sold at retail -- is where the business opportunity lies -- arbitraging the cost of content against the subscription charge. Actually that's the same thing newspapers did -- arbitraging the cost of syndicated content, wire service and original reporting and advertising production costs against what was charged advertisers and subscribers. It seems simple and obvious today because it settled out over a 100 years or more. It's what every business figures out -- how to mark up your ingredients to make a profit at retail. We simple have to work out the arbitrage in this new world. This system provide the mechanics; the arbitrage is up to the market.

So in this system, Big Brother is blind for other than session authentication and billing purposes.

This approach may not be supported by some publishers, who will want what Dave Gehring would call "second-party data" about who the people are clicking on their content. See:
http://newshare.com/ohare/gehring-voices-alignment.pdf
http://newshare.com/ohare/gehring-voices-alignment.pdf
However, if a publisher chooses to become a service provider, then they get access to all of the activity of their OWN users across the network, giving them, in effect, "First Party" data vastly broader than they have access to today -- but only for those people they have account relationships with. This provides a hook for accountability as to use of personal data, and a hook that can be audited by the ITE administration if necessary.

C. SPECIFIC ELEMENTS OF THE SERVICE

It follows the principle that if you want to "own" and get data about a user, you have to maintain an account relationship with them which makes you accountable both to them and to the ITE's rules. Otherwise, they are anonymized to you beyond their service class and home base and perhaps some other attributes shared on a permissioned basis.

1) Every click across the network that involves an exchange of value (a payment for an article or a reward for viewing or doing something) is logged to an authentication and logging service, which is seen by the system participants as a "central shared service" although in network practice it may be distributed and hierarchical as with DNS.

2) The logging service knows the user only by a unique alphanumeric identifier supplied by the user's "home base" at the start of that particular session. As a matter of policy, it the logging service shall not sell or provide clickstream data to ANYONE (including one hopes, the NSA, though I don't know how that can be assured) and provides it only to the user's home service provider for their purposes (and for audit purposes to the publishing content provider if requested). The identifer -- to anyone other than the home base itself. -- reveals nothing more than the identity of the user's home base to anyone else in the system other than the user's home base account manager.

3) There may be a plurality of home-base account managers in the service (as their are thousands of home bases in Shiboleth/Internet2), providing end users a high degree of choice regarding business terms, especially as to identity and privacy.

4) At settlement time, the settlement service bundles all the clicks -- sorted by home-base of the users on the one hand and by the vending publisher on the other hand -- and determines an aggregate debit or credit to charge the home base and an aggregated credit or debit to charge the publishers (note that a "publisher" could be a brand which is paying for a user to view a commercial message). This all is done periodically -- daily, weekly, monthly -- probably weekly in prototype -- across the bank ACH network.

5) The home base gets these bundled log reports and is free to sort them or use them as they wish (subject to their terms of service with the end user as to usage and privacy protection or not); in some cases there may be a discrete charge or payment to the end user for a particular access; in the vast majority of cases (I think) , the home base will use the click-stream reports for demographic, marketing and business-model analysis but the end user will merely be paying a monthly subscription for some class of service.

6) The publisher (or information service provider), also gets bundled log reports of total usage so they can audit their payment or receipts, and the only sorting they are capable of doing is by the source of the end-user (i.e., their service-provider ID). Conceivably they might have methods to associate these anonymized usage reports to specific users, but the ITE would be in the business of making business rules governing this practice and the rules would be enforceable by anything up to the ultimate sanction -- cutting the offending information service provider off the system.

7) The provision for non-regulatory sanctions is one of the reasons why the governance and ownership of the service is so critical. The cutoff decision has to be the result of well-documented interchange rules (consider Visa as a model in this regard), and the entity making the decision has to have no competitive business interest one way or the other but rather ony an interest in the fair administration of the service and due regard for evolving identity and privacy rights of end users. Hence, the need for a non-governmental and non-investor-owned entity with a mission to efficiently oversee and operate a service and not profit from it. Profit is for the publishers and service providers who use the service.

D. TWO STAKEHOLDER GROUPS

We might thus see two sets of stakeholders in the ITE:

- Technology and business service providers who operate ITE-sanction services under contract with the ITE, for which they pay some relative diminimus transaction- or volume-based license fee. These might include operators of the authentication and logging services, and providers of ancillary services that must interoperate with all auth and logging services. These might include financial-service firms which do settlement on records providing by the auth/logging service, as well as entities who act as authorized agents of either publishers or end-user service providers to perform business-case services on network data.

- Publishers/information service providers, and billing/subscription end-user service providers who wish to be authenticated across the entire ITE service network. Most of their cost would be payments to the tech and business-service providers of their choice (above) at free-market prices. But they would also be asked to pay an "interchange fee" based on transaction volume to the ITE, again solely sufficient to fund the ITE's governance and any necessary R&D. What they get for the interchange fee is a unique, ITE-wide identifier and the assurance they and their users will be "authenticated" globally so long as they play by the ITE's rules.