

anonymity, identity and the role of libraries & other info-mediaries



ian kerr

canada research chair
in ethics, law & technology

Université D' Ottawa University of Ottawa
Faculté de droit Faculty of Law

mary minow

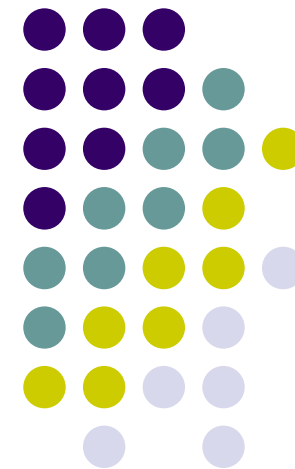
consultant

LibraryLaw.com

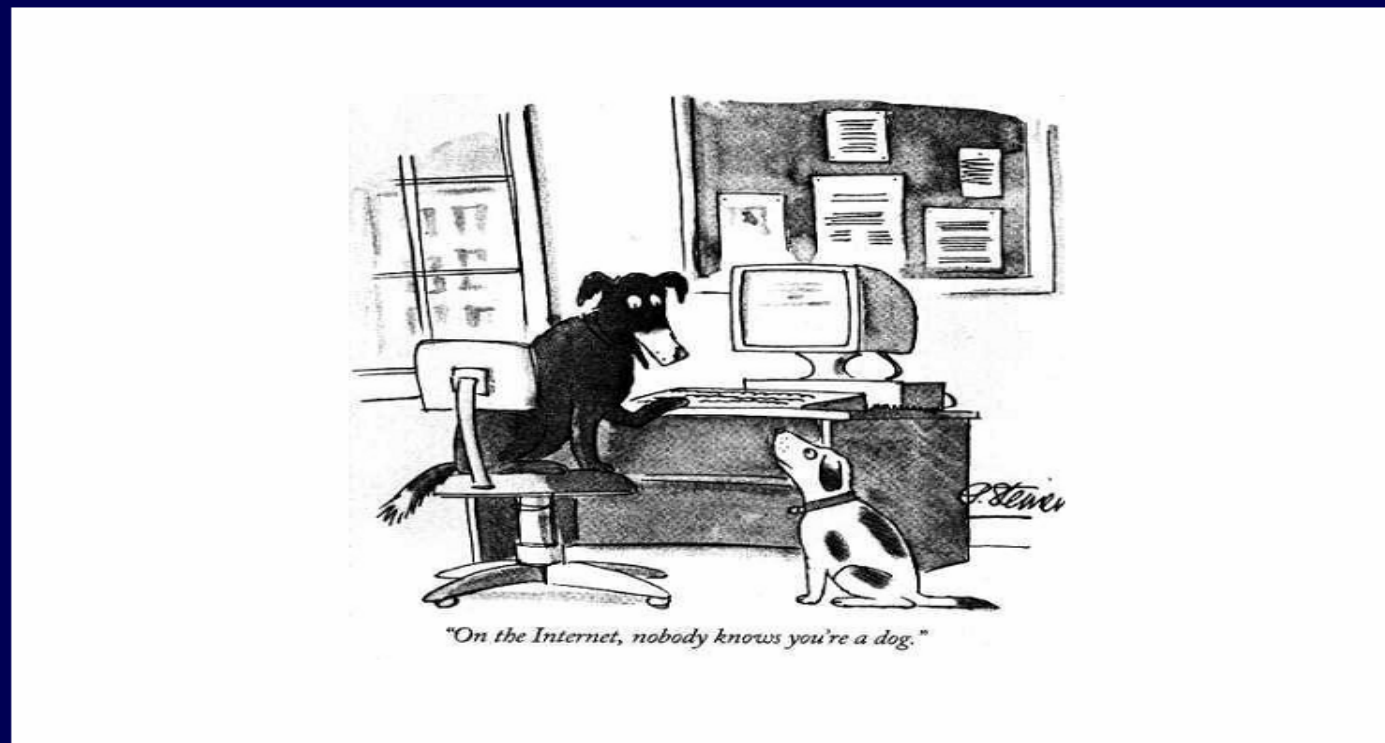
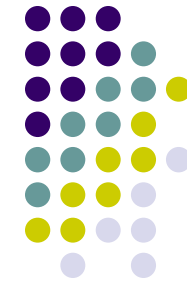
policy analyst

California Assoc. of Library
Trustees & Commissioners

technology law in canada's technology capital

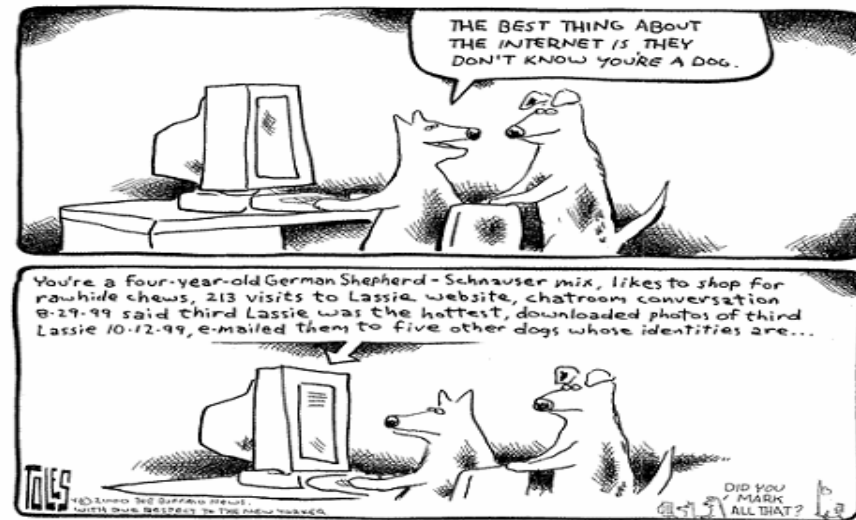


dognymity



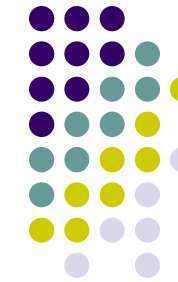
↑
July, 1993

dogthentication



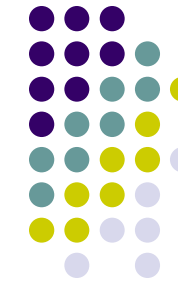
April, 2000

possible explanations



- surveillance is the cost of privacy (nock)
 - anonymity makes us strangers, and strangers are untrustworthy...
- ecommerce prefers authenticity
 - business proceeds best by establishing degrees of confidence about a stranger's identity, attributes, credentials or eligibility

is anonymity going to the dogs?



“i like the idea of anonymity in principle, but i think that when there is a good showing that an anonymous actor is engaged in illegal conduct you have a right to find out who they are”

- quiz: cary sherman (riaa)
or
lawrence lessig (stanford law)

????

is anonymity going to the dogs?



“i like the idea of anonymity in principle, but i think that when there is a good showing that an anonymous actor is engaged in illegal conduct you have a right to find out who they are”

- quiz: **cary sherman** (riaa)
or
lawrence lessig (stanford law)

!!!!

is anonymity going to the dogs?



“i like the idea of anonymity in principle, but i think that when there is a **good showing** that an anonymous actor is engaged in illegal conduct **you** have a **right** to find out who they are”

- quiz: cary sherman (riaa)
or
lawrence lessig (stanford law)

!!!!

the assault on anonymity (1)



- anonymity is generally dishonorable because it:
 - is the “refuge of scoundrels”
 - “facilitates wrong by **eliminating accountability**, which is ordinarily the very purpose of the anonymity.”
 - is “a distortion of the past that will lead to a coarsening of the future.”
 - per scalia j (dissenting, *mcintyre v. ohio elections commission*)

the assault on anonymity (2)



- need to recognize shifting base conditions (taipale)
 - changing nature of compelling state interest and balance of power
 - no longer “I am weak, state is strong”
 - asymmetric threats no longer puny
 - force multiplier effect of technology
 - changing nature & availability of alternative strategies
 - crypto, chained remailers, etc allow “true” anonymity
 - “no court order can break strong encryption”

shifting ground? (yeo)



“pay attention to what privacy advocates are saying ... and note how frequently these days one hears privacy advocates talking less and less about ...the right of privacy, and more and more about ... something like a right to anonymity. Moreover, note also how anonymity is increasingly spoken about as if ... winning the right to be anonymous (e.g., with respect to this or that research database) were the same as winning the right of privacy, as if a victory for anonymity were a victory for privacy, as if to advocate for anonymity were to advocate for privacy, etc.”

evidence? (lessig)



“a strong ethic and architecture of pseudonymous identity, properly protected, would give us more privacy than we have today”

freedogs (davidson)



“I shall not be wasting my time developing identity escrow systems nor launching revolutions against systems which others believe worthy of defending. Instead, I shall be continuing my work to develop, implement, and utilize free market money, bearer instruments with digital features, and absolute anonymity so that more people can break free of the various systems of control and enslavement and get on with their own business.”

cry for identity management policy (clarke)

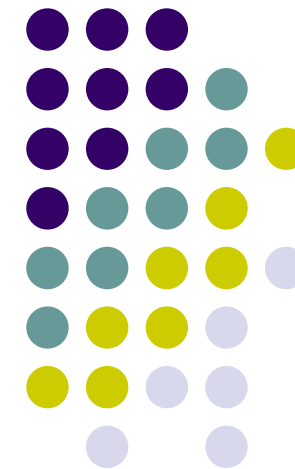


“what we need is a task force that blends the **technical** expertise, with the **legal** perspective and the **policy** perspective, with the aim of producing a series of white papers on effective pseudonymity services that will complement the anonymity services that are bound to exist in any case.”

on the identity trail



understanding the importance and
impact of anonymity and authentication
in a networked society



IDENTITY

on the trail



- *the context:*
privacy in the age of ubiquitous
computing and distributed intelligence

anon equity



- *the glue:*
a collective commitment to the idea that the **preservation of anonymity** is critical to the maintenance of a free and democratic society



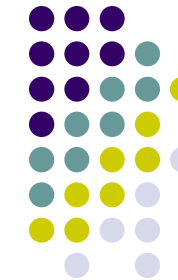
the anonymity project



- *our aim:*
to better understand the impact of information and authentication technologies on our identities, and on our ability to be anonymous



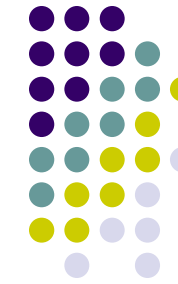
the anonymity project



- a multidisciplinary research project (SSHRC)
- academics, activists, businesses, educators, ethicists, NGOs, policy analysts, policy makers, private sector researchers
- promoting privacy research across a broad array of disciplines including:
 - philosophy
 - ethics
 - feminism
 - cognitive science
 - law
 - public policy
 - government
 - business
 - cryptography
 - engineering
- employing and training 80 students across Canada and US over a four year period



the anonymity project



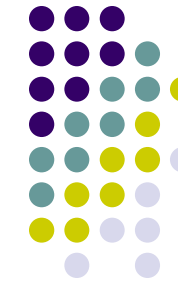
- 3 research tracks
 - t1 nature and value of anonymity, identity, and authentication
 - t2 constitutional, legal and policy aspects
 - t3 technologies that anonymize, identify, and authenticate

t1 nature and value of anonymity, identity, and authentication



- historical, philosophical, and psychological aspects
- epistemology and ethics
- perceptual experience of anonymity and identifiability
 - jacquie burkell (psych/cogsci)
 - steven davis (phil/cogsci)
 - marsha hanen (phil/feminism)
 - ian kerr (phil/law)
 - COVE; chumir foundation

t2 constitutional, law & policy aspects



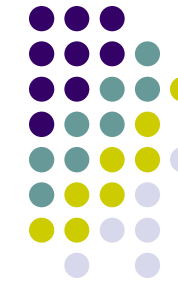
- role of constitutions and bills of rights
- privacy legislation
- law & policy in standards and architectures
- developing resources for public interest groups, communities and individuals
 - ken anderson / mary o'donoghue (law)
 - ann cavoukian (policy)
 - jane doe (activist)
 - daphne gilbert (law)
 - guy herriges (policy)
 - ian kerr (law)
 - pippa lawson (law)
 - stephanie perrin (policy)
 - marc rotenberg (law)
 - OIPC; EPIC; CIPPIC

t3 technologies that identify, anonymize and authenticate



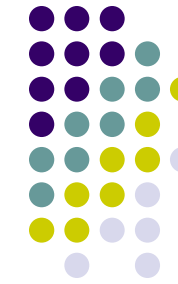
- secure private credentials
- secure electronic voting systems
- wearable computing
 - stefan brands (cryptography)
 - david chaum (cryptography)
 - steve mann (electrical engineering)

nyms 101 basic categories (a la clarke)



- identified record/transaction
 - data trail can be readily related to a particular individual (either directly or when linked to other available data)
- anonymous record/transaction
 - data trail cannot be associated with a particular individual (even when linked to other available data)
- pseudonymous record/transaction
 - data trail cannot, *in normal course of events*, be associated with a particular individual

nyms 101 privacy vs. confidentiality



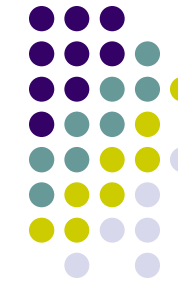
- **informational privacy**
 - interest/expectation/right that individuals ought to be able to control information about themselves
- **confidentiality**
 - interest/expectation/right that a trusted third party will not reveal personal information about an individual
(or will only reveal under restricted conditions)

disintermediation



- distribution models // information flows
- info-mediaries

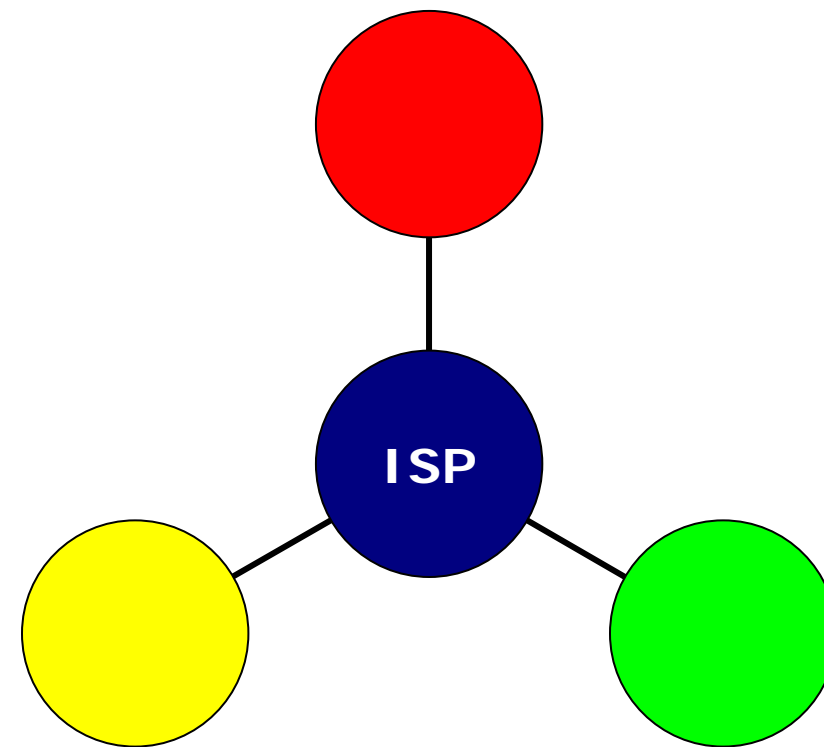
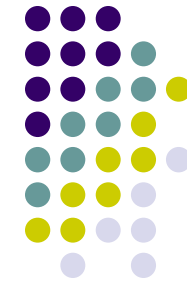
the unenviable position of isps



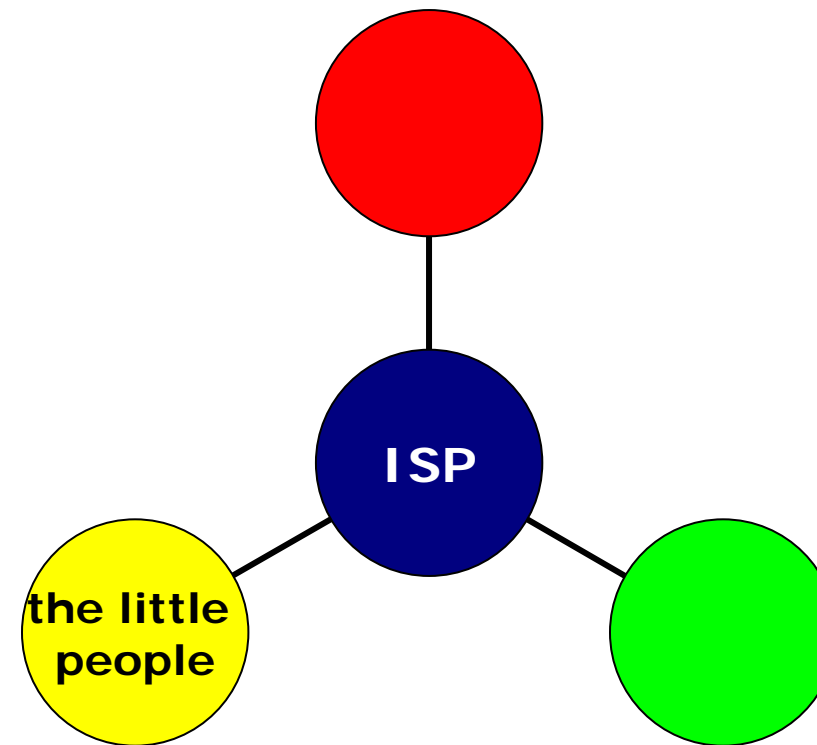
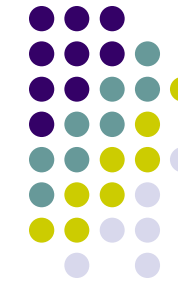
A determination of the scope of liability of network operators will surely have ramifications on freedom of speech. If computer operators are held liable for the expression of their subscribers it would place a duty on them ... The result would likely lead to **an increase in screening of private messages**. It would potentially **result in censorship**, as companies would wish to protect themselves from possible civil or criminal liability. This would put network administrators in **the unenviable position of deciding what is acceptable speech** and what is not.

Sopinka J. (1997)

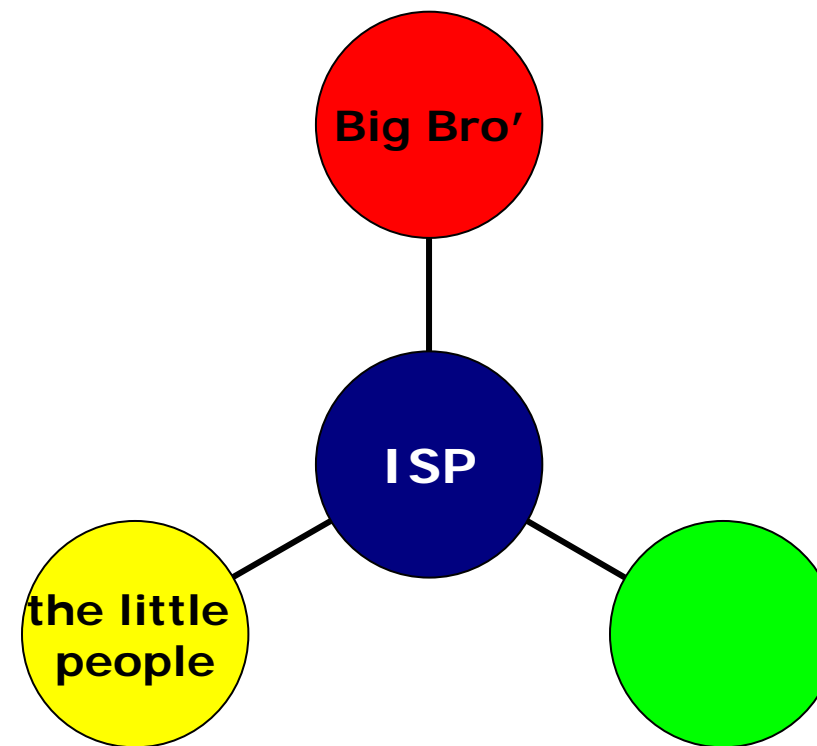
The Internet's Strange Chemistry



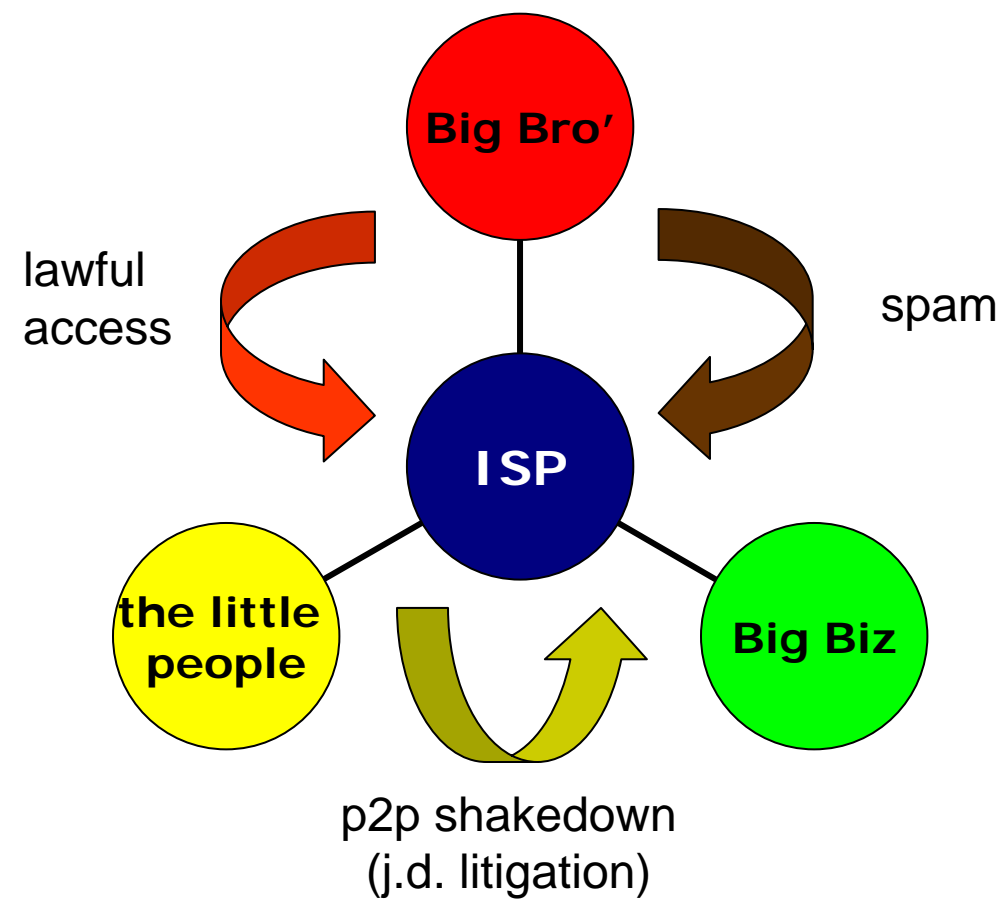
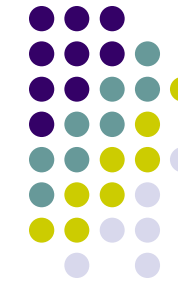
The Internet's Strange Chemistry



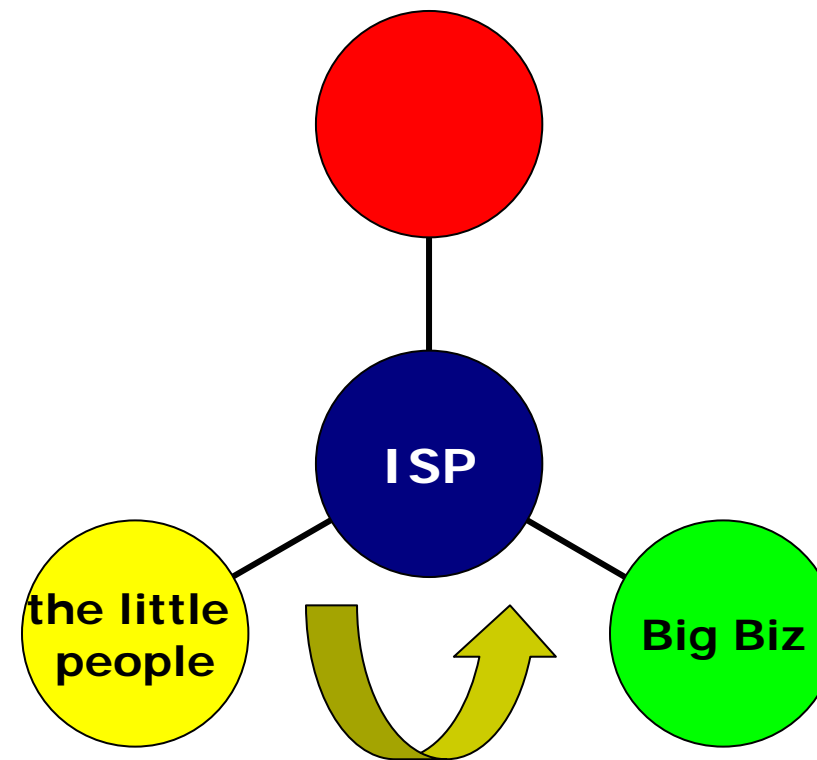
The Internet's Strange Chemistry



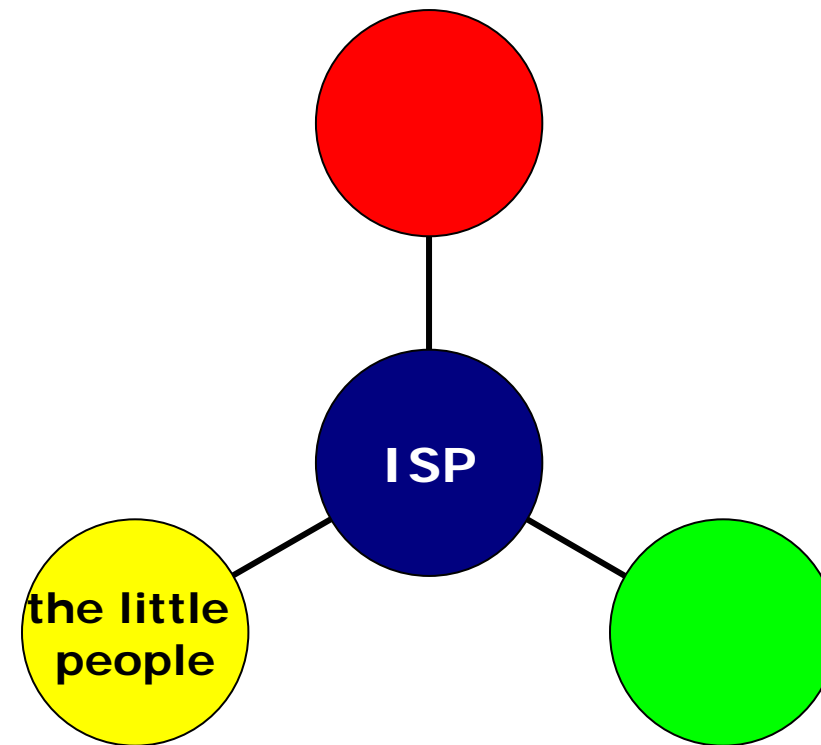
The Internet's Strange Chemistry



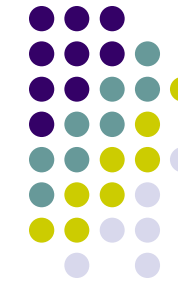
The p2p Shakedown (j.d.)



ISPs & The Little People



bmg v doe (cria case)



- not just a copyright case
- *parties* - 17 cria companies; 29 j.does; 5 isps; 2 interveners
- *what cria sought* - last known names; home mailing address; business address; telephone numbers; fax numbers; email addresses and copies of isp records
- *what cria thought it knew* (ie, hired a surveillance company who *said* it knew...) - p2p pseudonyms; ip addresses
- *what cria knew it didn't know* - whether the downloaded files were actually cria-owned content; whether the person named in the subscriber account could be linked to the alleged wrongdoing (lans; wi-fi); whether the info sought from isps linking ip addresses to subscriber accounts was reliable

bmg v doe (2)



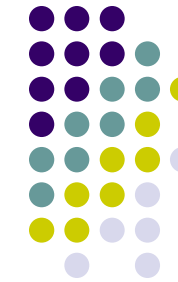
- *cria argued* - defendants had no reasonable expectation of privacy:
 - the nature of the isp-user relationship is commercial
 - any expectation of privacy would not extend to remaining anonymous in light of evidence of their copyright infringements
- *other parties argued* - that adopting *cria* position would amount to a civil search warrant with no legal process to protect the targets of the litigation; very high threshold test required before court should order disclosure
- *court held* – information requested must be: minimal and reliable; privacy concerns *in this case* outweigh public interest in favor of disclosure b/c of serious risk of innocent subscriber privacy interests might be breached

bmg v doe (3)



- *moral of the story* for plaintiffs
 - plaintiffs must come to court with solid evidence of:
 - actual wrongdoing
 - a reliable link between the alleged wrongful activities and specific individuals
- *moral of the story* for isps & defendants ...?!

relationships of dependence



- social exchange theory
participants in a social interaction jointly determine the rewards and costs that they achieve from it
- dependence
the degree to which one of the two interacting parties needs their relationship
(i.e., X's outcomes are affected by the relationship)

relationships of dependence



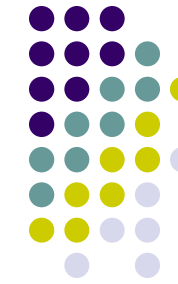
- ↑ favourable outcomes ↔ ↑ dependence
- ↓ alternative relationships ↔ ↑ dependence
- ↑ investment of resources ↔ ↑ dependence

power



- is fundamentally rooted in the dependence actors have on one another
- the potential for one actor to obtain favourable outcomes in an exchange episode at another's expense
- the extent to which one person, by varying her behaviour, can affect the quality of another's outcomes

two types of power



- **behaviour control**

X's power to vary Y's outcomes is reduced through Y's decision to modify his or her behaviour

- **fate control**

X has the power to vary Y's outcomes regardless of what Y does

internet user dependence



- users need ISPs to gain access
(users dependent, so long as they lack resources & alternatives)
- users need ISPs to take proper care and control of their personal information and private communications
(users dependent, so long as ISP's are able to collect and disclose user information)

internet user dependence



- the ability to disclose user information empowers ISPs with both **behaviour** and **fate** control
- e.g., by disclosing personal information to RIAA/CRIA an ISP has the power to vary user outcomes
- exercise of such power may become problematic when a user has reposed confidence or trust in an ISP

relationships of trust & confidence



- there is longstanding judicial recognition that the preservation of society requires the protection of **trusting relationships**
- the leeway afforded to the **fiduciary** to affect the legal position of the **principal** puts the latter at the mercy of the former
- of concern:
trusted parties may serve their own ends rather than those of the trusting party

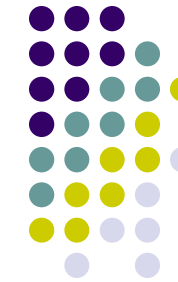
relationships of trust & confidence



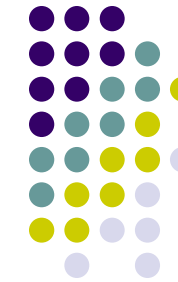
- this necessitates the existence of a legal device which will induce the fiduciary to use his power beneficially
- the **fiduciary obligation** is law's realization of the social importance of protecting relationships of dependence
- the imposition of a **fiduciary obligation** serves to protect those who have come to depend on others by **legally** reposing trust in them

status based fiduciaries

- trustee/beneficiary
- solicitor/client
- principal/agent
- director/corporation
- employer/employee
- guardian/ward
- doctor/patient
- parent/child



fact-based fiduciaries



- wilson j.'s "rough and ready guide" in *frame v. smith*
 - (1) the fiduciary has scope for the exercise of some discretion or power
 - (2) the fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal or practical interests
 - (3) the beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary holding the discretion or power

fact based fiduciaries (2)

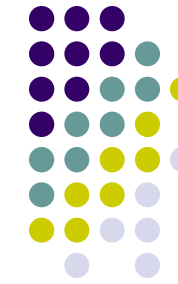


- la forest j.'s 'fiduciary expectation' in *hodgkinson v. simms*

...the question to ask is whether, given all the surrounding circumstances, one party could reasonably have expected that the other party would act in the former's best interests with respect to the subject-matter at issue.

Discretion, influence, vulnerability and trust [are] non-exhaustive examples of evidential factors to be considered in making this determination.

ISP-user relationships



- ISPs have unparalleled access to their users' informational assets
- an ISP acting *male fides* might:
 - convert a user's personal information or private communications to its own advantage
 - disclose information without authority to a competitor or third party
 - turn over otherwise privileged evidence in the course of criminal or private litigation
- trusting users are therefore at the mercy of their ISP's unilateral exercise of discretion

ellison's vision



- NCs // PCs
- \$200 // \$2000
- **how?** basic input/output system that downloads a complete operating system when switched on
- all programs are downloaded from the network
- personal data files and backups are stored on servers connected to the system
- this allows users to slide a card into any NC and instantly begin work, as if the user were at home using her own machine
- **Gmail**

ISP-user relationships



- *the wrong Q*: are ISPs fiduciaries?
- *a better Q*: is an ISP *ever* a fiduciary?
- *an interesting Q*:
 - if an ISP were to act *as if* it were a fiduciary, what obligations might it owe to its users in the context of court proceedings? (aquacool2000; verizon)

anonymity, identity and the role of libraries & other info-mediaries



iankerr@uottawa.ca

canada research chair
in ethics, law & technology
Université D' Ottawa University of Ottawa
Faculté de droit Faculty of Law

