Identity and anonymity

Lorrie Faith Cranor

October 29, 2013

8-533 / 8-733 / 19-608 / 95-818:
Privacy Policy, Law, and Technology

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Identifiers

- Labels that point to individuals
  - Name
  - Social security number
  - Credit card number
  - Employee ID number
  - Attributes may serve as (usually weak) identifiers (see next slide)
- Identifiers may be “strong” or “weak”
  - Strong identifiers may uniquely identify someone while weak identifiers may identify a group of people
  - Multiple weak identifiers in combination may uniquely identify someone
  - Identifiers may be strong or weak depending on context

Attributes

- Properties associated with individuals
  - Height
  - Weight
  - Hair color
  - Date of birth
  - Employer

Identity

- The set of information that is associated with an individual in a particular identity system
- Individuals may have many identities

Identification

The process of using claimed or observed attributes of an individual to determine who that individual is

Authentication

- About obtaining a level of confidence in a claim
  - Does not prove someone is who they say they are
- Types
  - Individual authentication
  - Identity authentication
  - Attribute Authentication
- Three approaches
  - Something you know
  - Something you have
  - Something you are

Credentials or authenticators

Evidence that is presented to support the authentication of a claim

Authorization

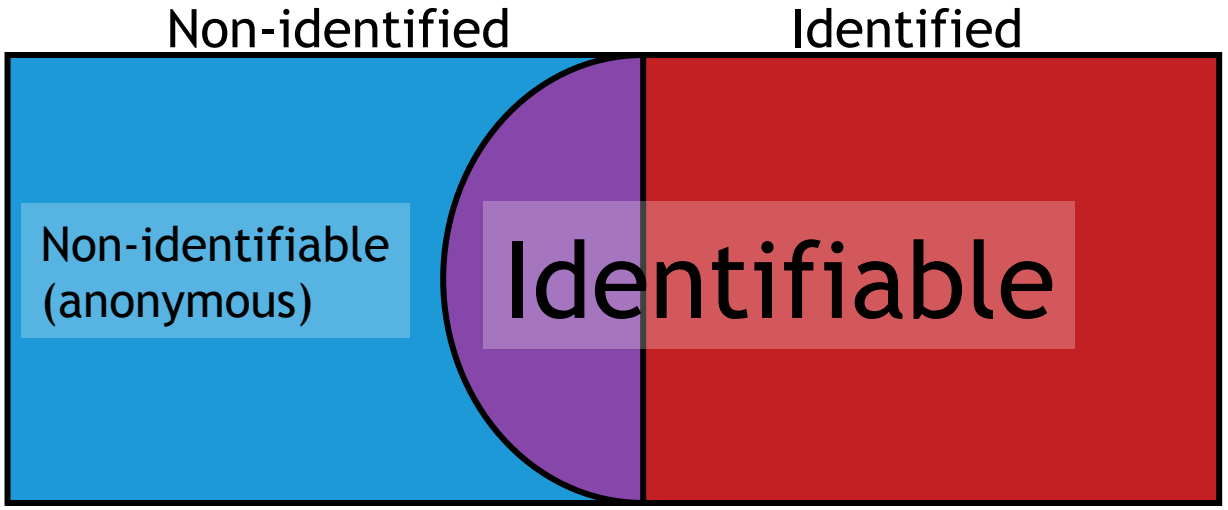
The process of deciding what an individual ought to be allowed to do

What does it mean to be identifiable?

Identifiable person (EU directive): “one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”

Identifiable vs. identified

- P3P spec distinguishes identifiable and identified
- Any data that can be used to identify a person is identifiable
- Identified data is information that can reasonably be tied to an individual



How unique are you?

- http://aboutmyinfo.org

Linkable vs. linked

- P3P requires declaration of data linked to a cookie
- Lots of data is linkable, less data is actually linked
- Where do we draw the line? Draft P3P 1.1 spec says:
  - A piece of data X is said to be linked to a cookie Y if at least one of the following activities may take place as a result of cookie Y being replayed, immediately upon cookie replay or at some future time (perhaps as a result of retrospective analysis or processing of server logs):
    - A cookie containing X is set or reset.
    - X is retrieved from a persistent data store or archival media.
    - Information identifiable with the user -- including but not limited to data entered into forms, IP address, clickstream data, and client events -- is retrieved from a record, data structure, or file (other than a log file) in which X is stored.

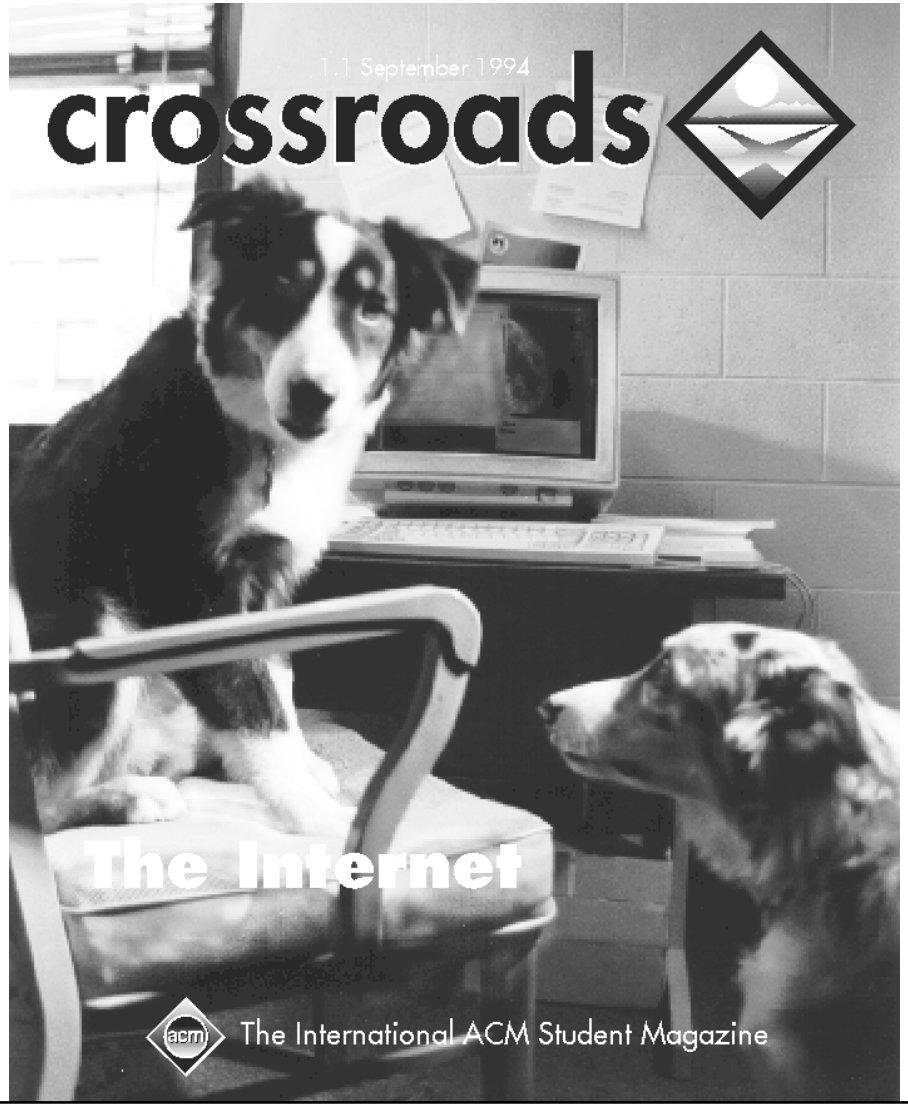
Privacy and identification/ authentication

- To better protect privacy:
  - Minimize use of identifiers
    - Use attribute authentication where possible
  - Use local identifiers rather than global identifiers
  - Use identification and authentication appropriate to the task

Cartoon dogs are anonymous on the Internet

"On the Internet, nobody knows you're a dog."

Real dogs are anonymous on the Internet too!



The Internet can’t be censored

“The Net treats censorship as damage and routes around it.”

- John Gillmore

Actually, none of this is true

- Easy to adopt a pseudonym on the Internet
- But difficult to be truly anonymous
  - Identities can usually be revealed with cooperation of ISP, local sys-admins, web logs, phone records, etc.
- The Internet can put up a good fight
- But there is still a lot of Internet censorship
  - Repressive governments and intellectual property lawyers have been pretty successful at getting Internet content removed

Degrees of anonymity

More

- Absolute privacy: adversary cannot observe communication
- Beyond suspicion: no user is more suspicious than any other
- Probable innocence: each user is more likely innocent than not
- Possible innocence: nontrivial probability that user is innocent
- Exposed: adversary learns responsible user
- Provably exposed: adversary can prove your actions to others

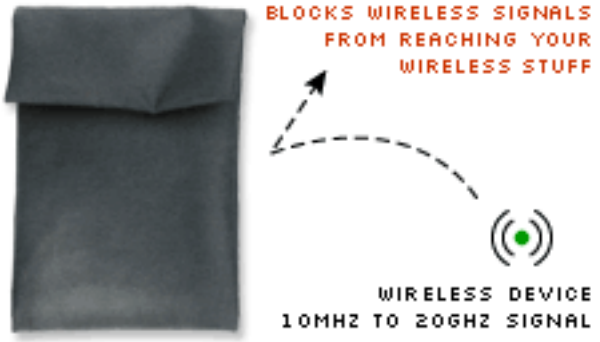
Less

Reiter, M. K. and Rubin, A. D. 1999. Anonymous Web transactions with Crowds. *Commun. ACM* 42, 2 (Feb. 1999), 32-48. DOI= http://doi.acm.org/10.1145/293411.293778

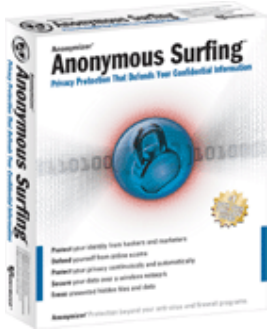
Anonymity tool applications

- Communication
- Publishing
- Payments
- Voting
- Surveys
- Credentials

Privacy Enhancing Technologies



http://www.mobilecloak.com/



http://tor.eff.org/

SECURITY SHREDDER SCISSORS | Dept 60319

(#96385)

___Security Shredder Scissors(s) @ $12.97 $

CA residents must add 7.25% sales tax $

Add Shipping & Handling ~~$3.95~~ FREE

Please Print Clearly

TOTAL $

SEND ORDER TO: **Dream Products, Inc.** 412 DREAM LANE, VAN NUYS, CA 91496

❑Check or money order **payable** to: **Dream Products, Inc.**

Charge my: ❑ VISA ❑ MasterCard ❑ Discover®/NOVUS℠Cards

Card# Expiration Date ___/___

Name _____

Address _____

City _____ ST ___ Zip _____

FOIL IDENTITY THIEVES WITH 5-BLADE SHREDDER SCISSORS

Guard personal information and identity with easy-to-use 5-blade Security Shredder Scissors. No need for noisy shredding machines. Razor-sharp stainless steel blades slice and shred bank statements, receipts, old checks, private communications… even credit cards with ease. Great for home or office. 7" long with molded comfort handles. Hurry, order today and get FREE Shipping & Handling!

Satisfaction Guaranteed or Return For Your Money Back

KEEP PRIVATE INFORMATION PRIVATE

www.DreamProductsCatalog.com (website offers may vary)

Delaware Lottery Games

Winning Numbers | Games | Where to Buy | Players Club | Claim Prizes | Rules
Winners | News + Events | Media Center | FAQs | For Retailers | Financials

search delottery.com GO

When you win, we won't tell a soul.
(You may have a harder time.)

When you win with the Delaware Lottery, privacy is our policy. We'll never release your name for promotional purposes - unless you tell us otherwise. Which means you can keep your good fortune as quiet as you want. So play Delaware Lottery Games. Because when you win big in our state, we won't say a word.

Click Here To Download Our "Guide To Winning Kit."

Kit includes: Guide To Winning Brochure, Mask Print Out, and Drawing Schedule

You could be the next winner?

Back to Top

Home | Contact Us | Directions | Site Map | Privacy Policy | Delaware State Government

Tell a Friend Sign up for Winning Number e-mails Play Responsibly

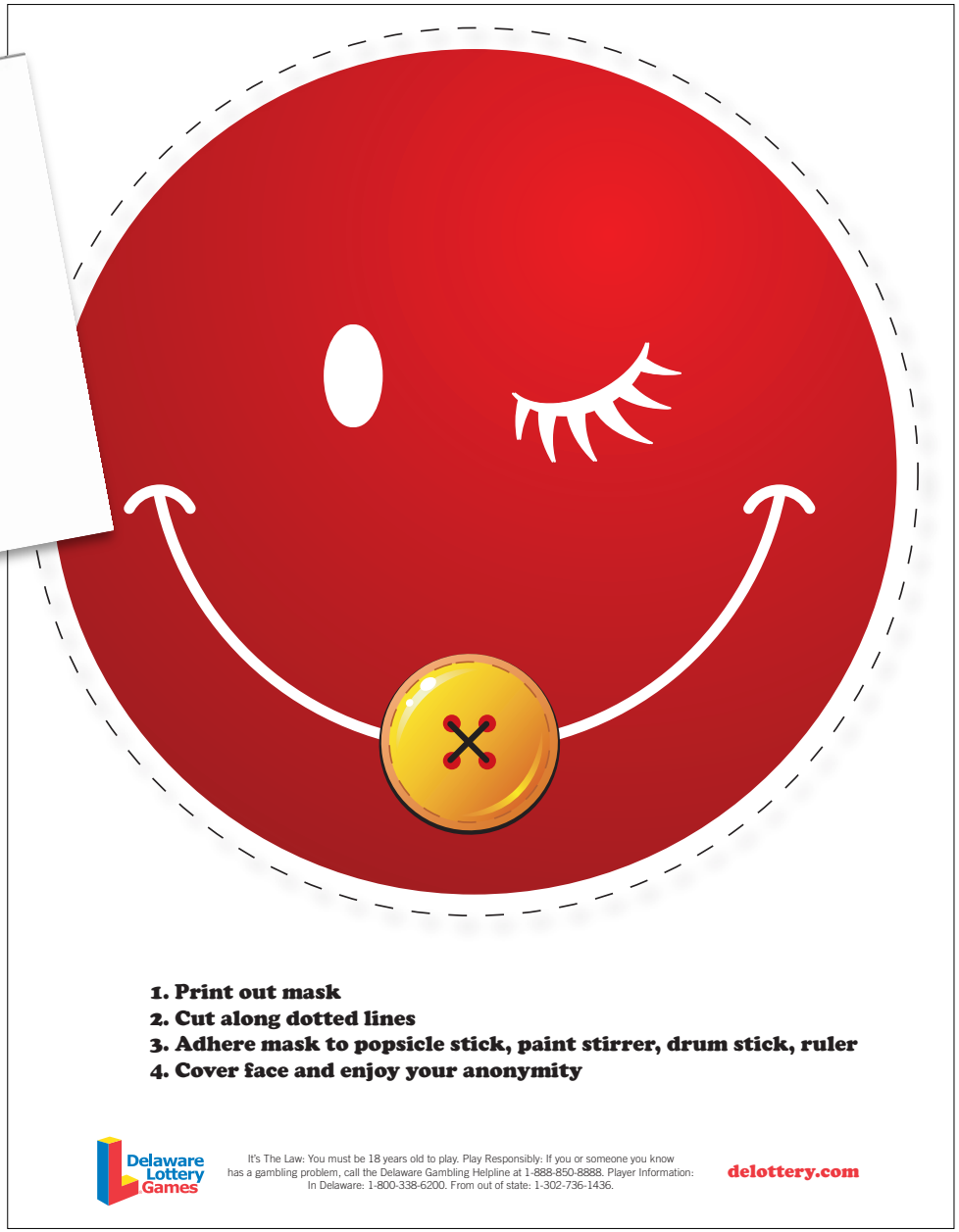
Wayne Lemons,
Delaware Lottery Director

Delaware Lottery Office
McKee Business Park
1575 McKee Road, Suite 102
Dover, DE 19904
Phone: 302-739-5291
Fax: 302-739-6706

Play Responsibly — If you or someone you know has a gambling problem, call the Delaware Gambling Helpline — 1-888-850-8888.

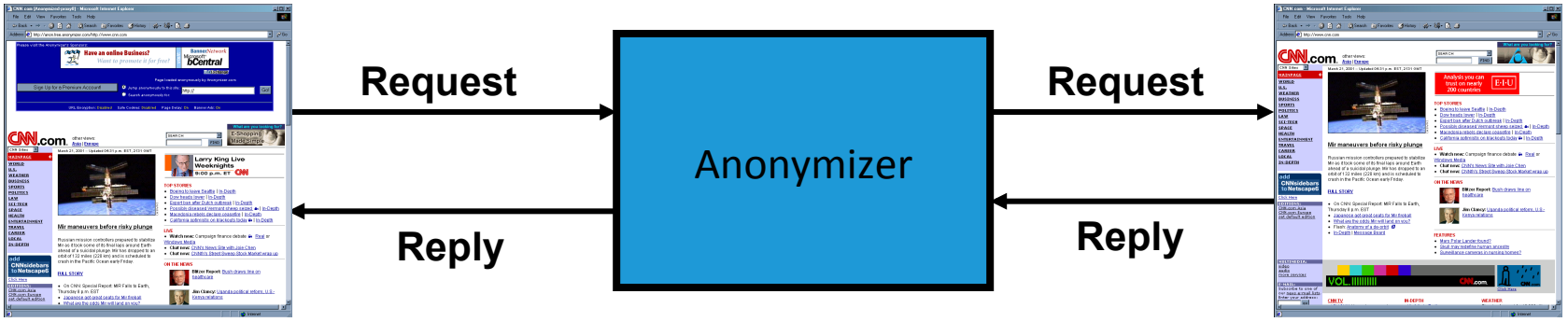
It's the Law — You must be 18 years of age or older to purchase Delaware Lottery tickets.

Designed to comply with the accessibility guidelines developed through the WAI and the Web Presentation Guidelines for State of Delaware Agencies.



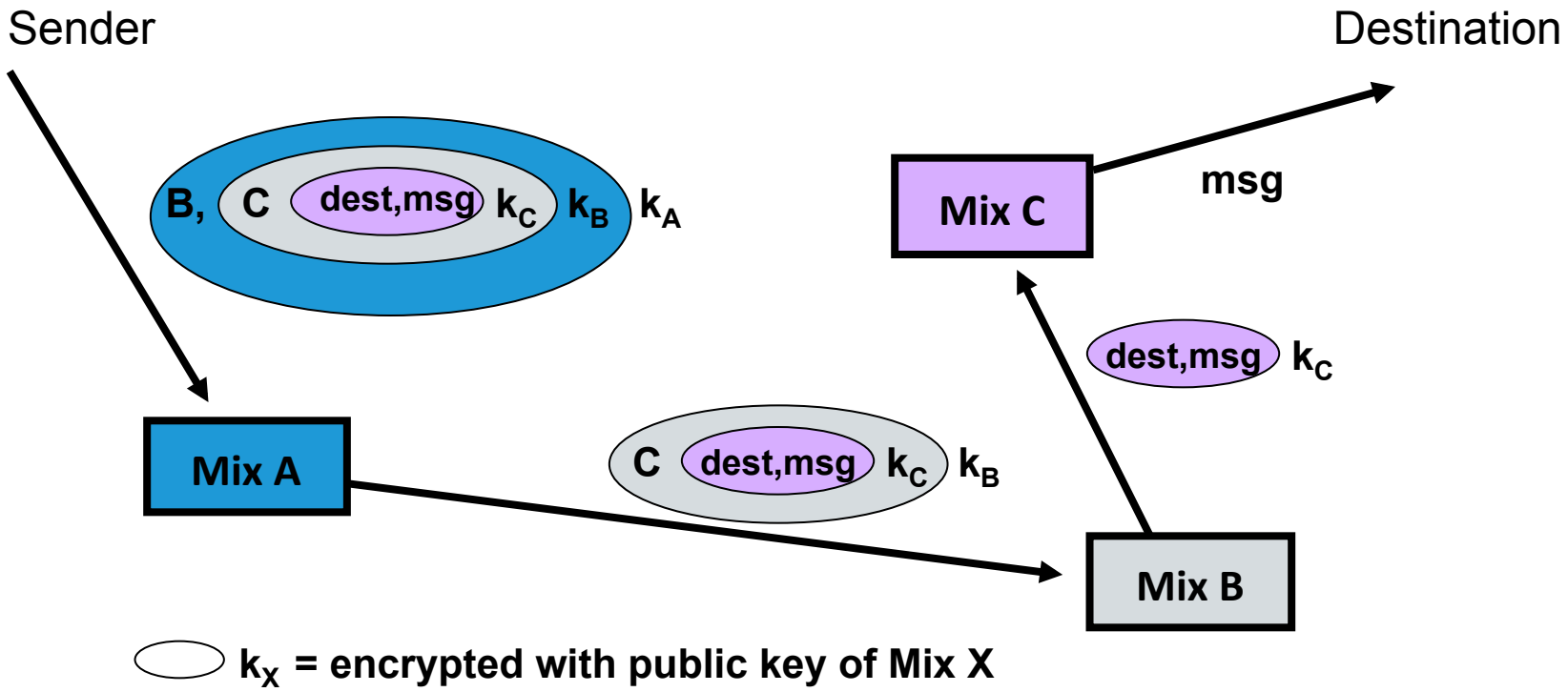
1. Print out mask
2. Cut along dotted lines
3. Adhere mask to popsicle stick, paint stirrer, drum stick, ruler
4. Cover face and enjoy your anonymity

The Anonymizer

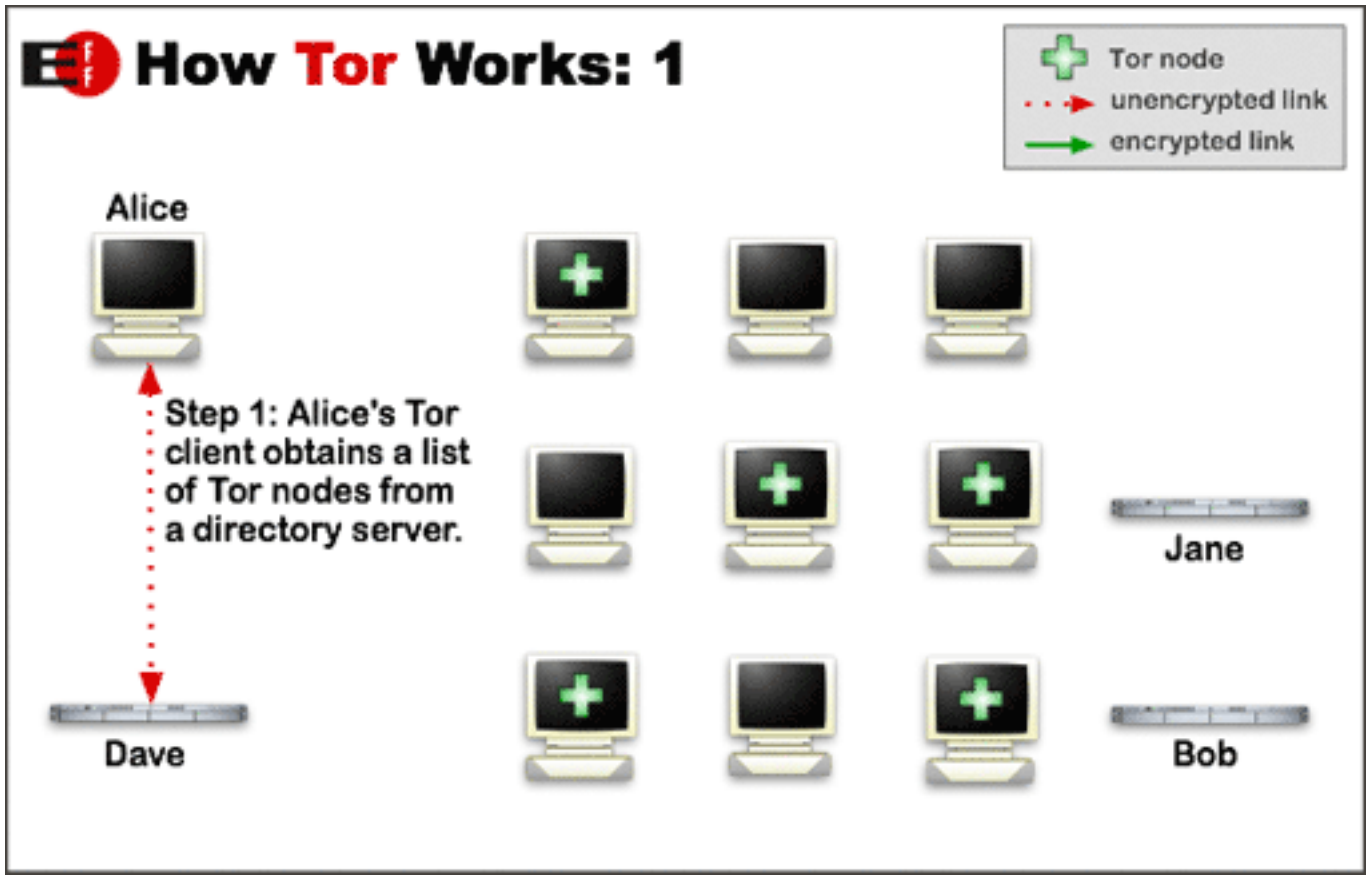


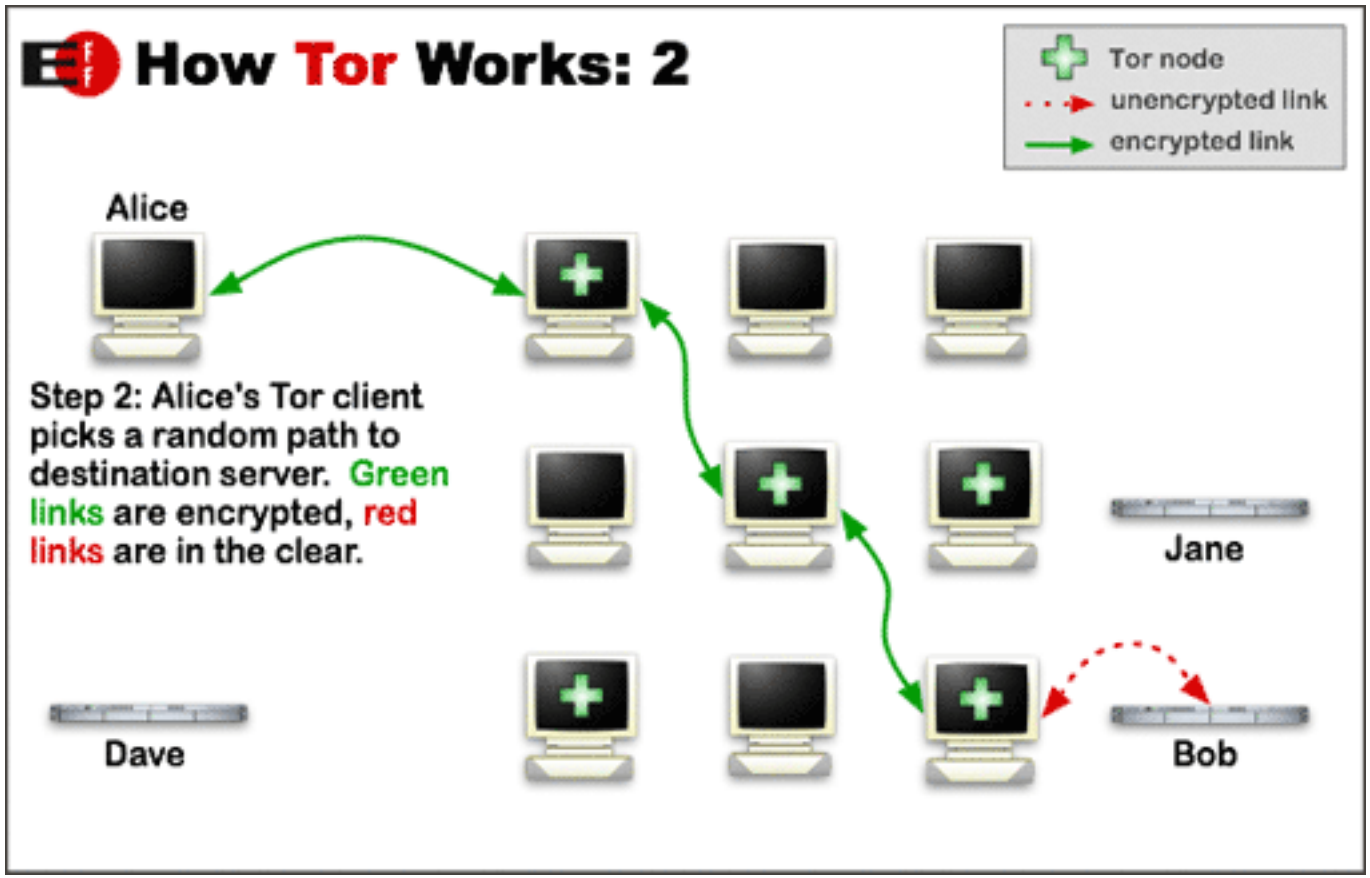
- Acts as a proxy for users
- Hides information from end servers
- Sees all web traffic
- Adds ads to pages (free service; subscription service also available)
- http://www.anonymizer.com

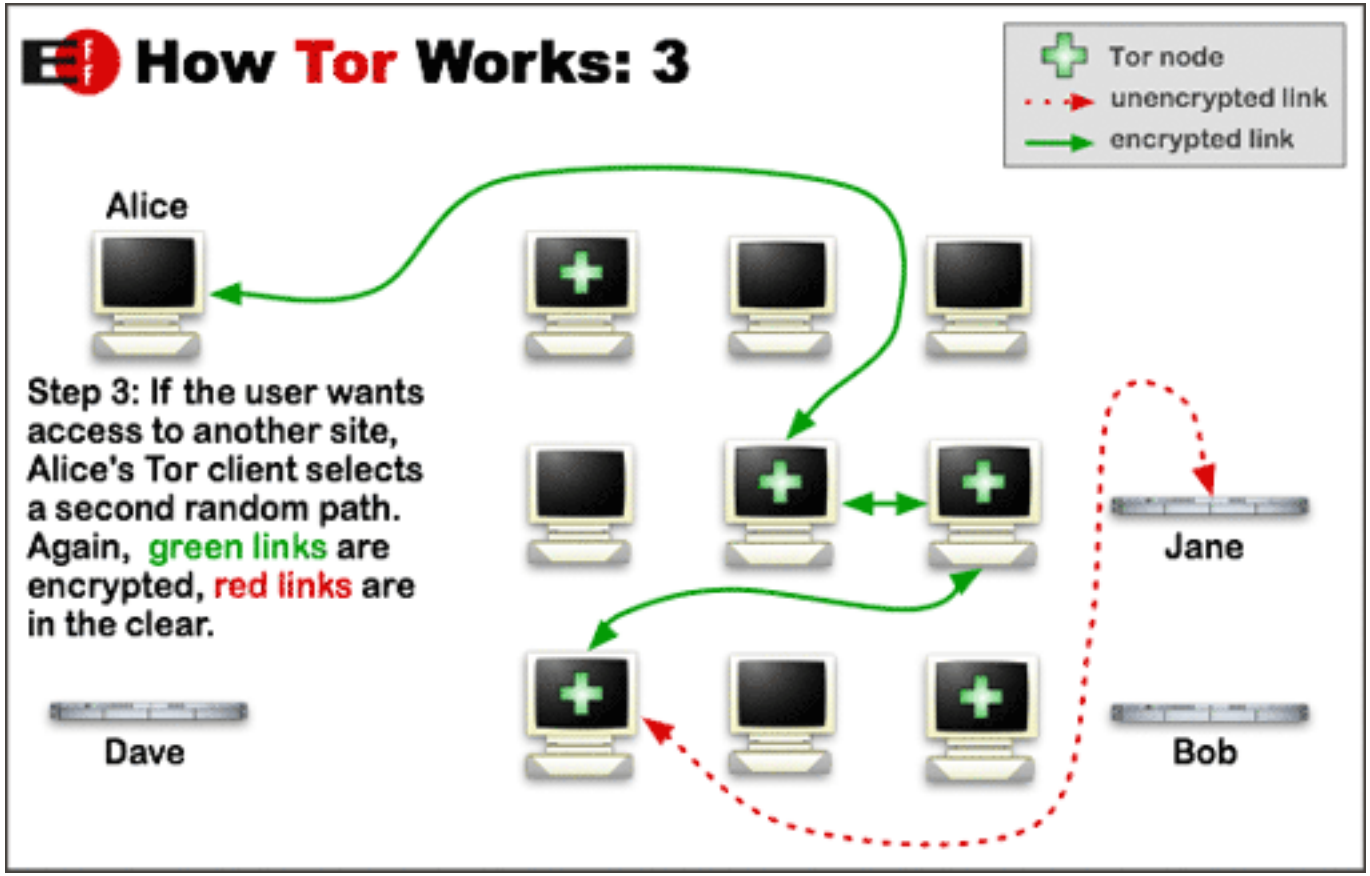
Mixes [Chaum81]



Sender routes message randomly through network of “Mixes”, using layered public-key encryption.


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

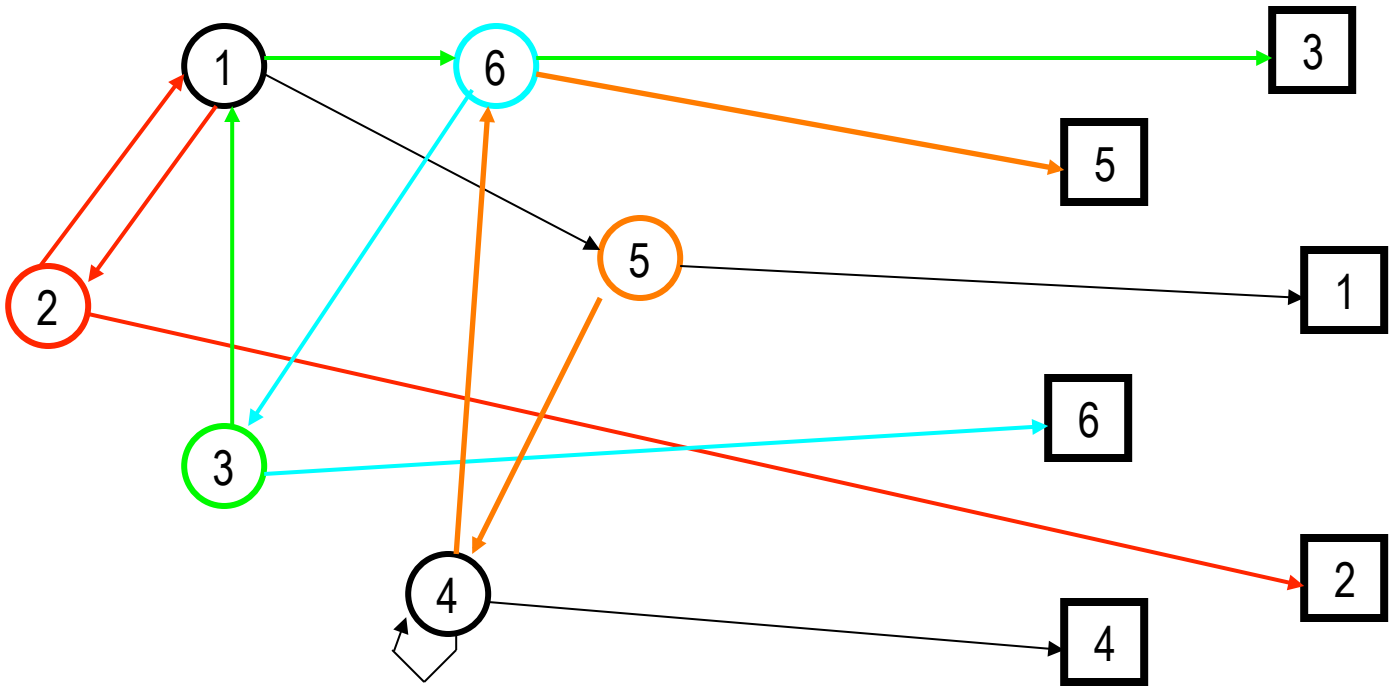

How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Crowds

- Users join a Crowd of other users
- Web requests from the crowd cannot be linked to any individual
- Protection from
  - end servers
  - other crowd members
  - system administrators
  - eavesdroppers
- First system to hide data shadow on the web without trusting a central authority

Crowds



Anonymous email

- Anonymous remailers allow people to send email anonymously
- Similar to anonymous web proxies
  - Send mail to remailer, which strips out any identifying information
- Some can be chained and work like mixes

Anonymous censorship-resistant publishing

- The printing press and the WWW can be powerful revolutionary tools
  - Political dissent
  - Whistle blowing
  - Radical ideas
- But those who seek to suppress revolutions have powerful tools of their own
  - Stop publication
  - Destroy published materials
  - Prevent distribution
  - Intimidate or physically or financially harm author or publisher

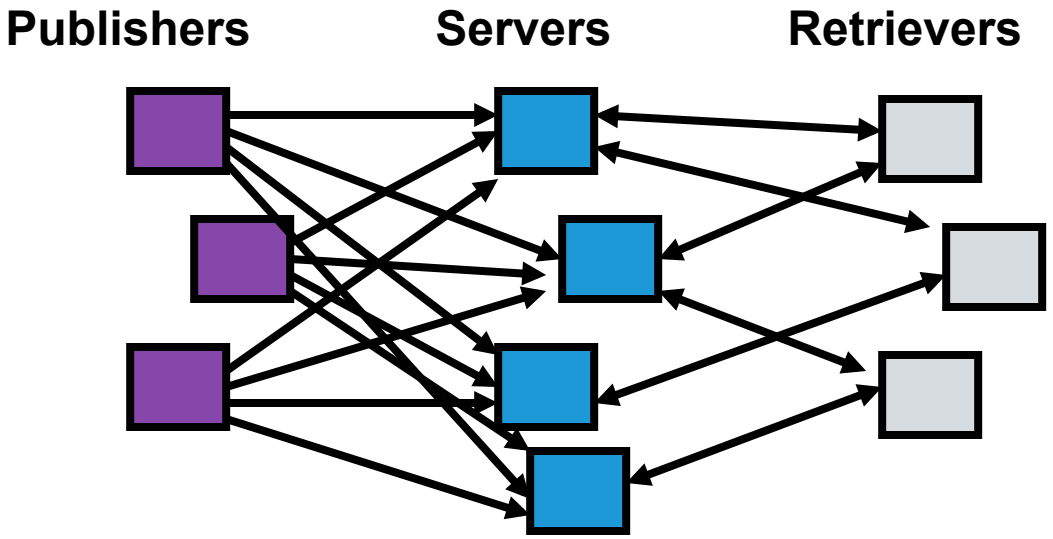
Anonymity increases censorship-resistance

- Reduces ability to force “voluntary” self-censorship
- Allows some authors to have their work taken more seriously
  - Reduces bias due to gender, race, ethnic background, social position, etc.
- Many historical examples of important anonymous publications
  - In the Colonies during Revolutionary War when British law prohibited writings suggesting overthrow of the government
  - Federalist papers

Publius design goals

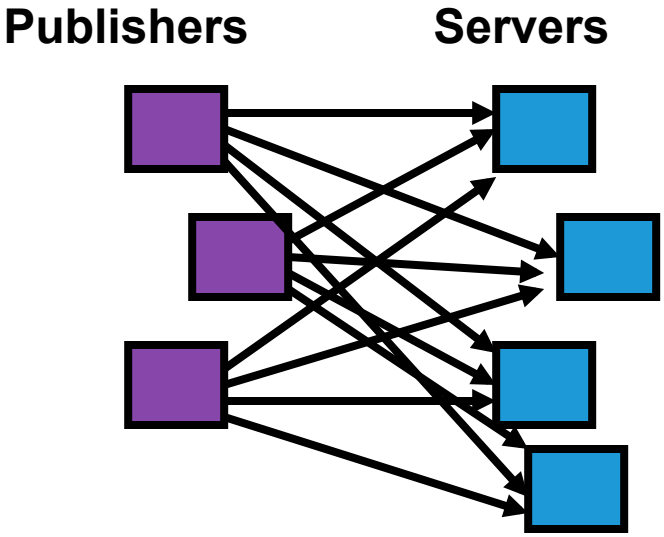
- Censorship resistant
- Tamper evident
- Source anonymous
- Updateable
- Deniable
- Fault tolerant
- Persistent
- Extensible
- Freely Available

Publius Overview



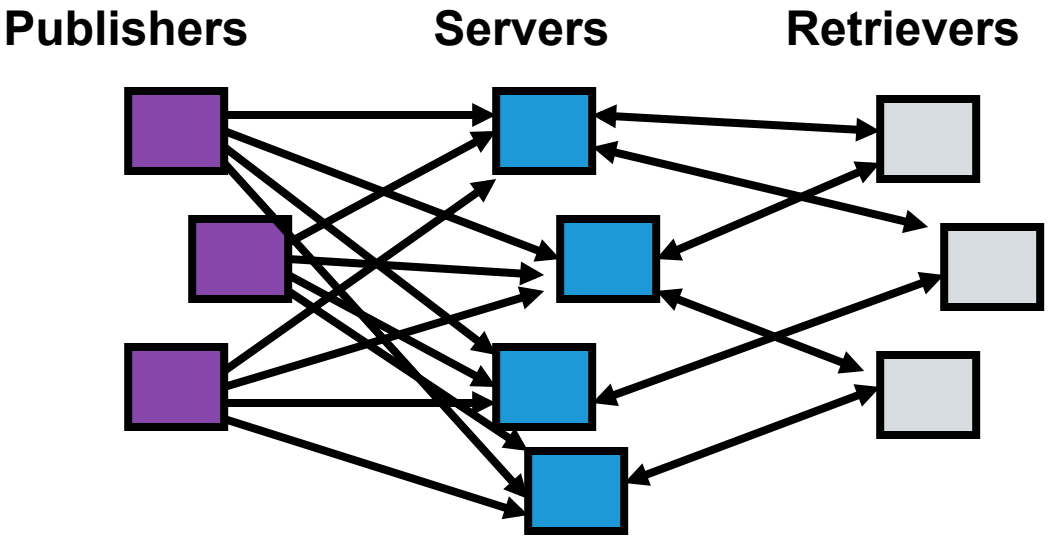
- Publius Content – Static content (HTML, images, PDF, etc)
- Publishers – Post Publius content
- Servers – Host Publius content
- Retrievers – Browse Publius content

Publishing a Publius document



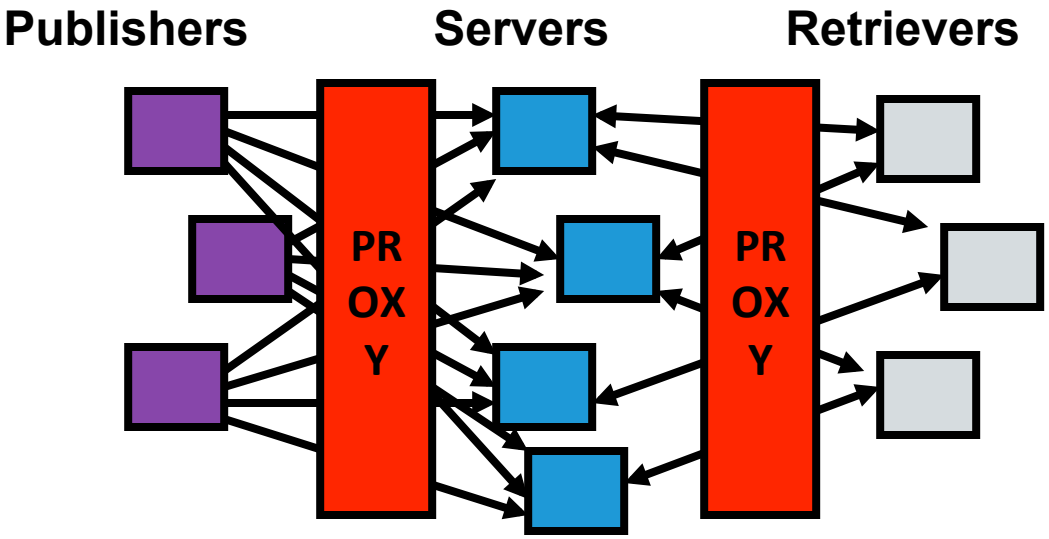
- Generate secret key and use it to encrypt document
- Use "secret splitting" to split key into n shares
  - This technique has special property that only k out of n shares are needed to put the key back together
- Publish encrypted document and 1 share on each of n servers
- Generate special Publius URL that encodes the location of each share and encrypted document – example: http://!publius!/ 1e6adsg673h0==hgj7889340==345lsafdfg

Retrieving a Publius document



- Break apart URL to discover document locations
- Retrieve encrypted document and share from k locations
- Reassemble key from shares
- Decrypt retrieved document
- Check for tampering
- View in web browser

Publius proxies



- Publius proxies running on a user's local machine or on the network handle all the publish and retrieve operations
- Proxies also allow publishers to delete and update content

Threats and limitations

- Attacks on server resources
  - 100K Content Limit (easy to subvert)
  - Server limits # of files it will store
  - Possibility: use a payment scheme
- Threats to publisher anonymity
- "Rubber-Hose Cryptanalysis"
  - Added "don't update" and don't delete bit
- Logging, network segment eavesdropping
- Collaboration of servers to censor content
  - A feature?

The Washington Post

SINESS

E

Stocks

FRIDAY, JUNE 30, 2000

Online and Unidentifiable?

AT&T Labs' 'Publius' System Aims to Return Anonymity to Posters

By JOHN SCHWARTZ
Washington Post Staff Writer

Everyone knows two things about the Internet. First, it's impossible to censor. Second, the Internet is anonymous.

As it happens, neither is true: The increasing ability to trace Internet surfers' wanderings and the threat of lawsuits have considerably dampened the online medium's Wild West spirit.

But that hasn't stopped people from trying to help the Net live up to its reputation. Today researchers at AT&T Labs will announce the creation of Publius, a new system that could go a long way toward eliminating online censorship. The innovation could bring the full promise—and, critics warn, the perils—of unfettered speech to the global medium.

"It seems like more and more, technologies are being introduced that limit the freedom of individuals—especially in repressive administrations" around the world, said Aviel D. Rubin, who developed Publius with AT&T colleague Lorrie F. Cranor and graduate student

See PUBLIUS, *E11, Col. 1*

BY TING-LI WANG FOR THE WASHINGTON POST

Creators Cranor, Rubin and Waldman intend their computer system to assist free speech, especially abroad.

Peer to Peer:

We've Only Just Begun

New distributed networks promise anonymous, censorship-proof posting. Is that a good thing?

BY ELINOR ABREU

Waldman, Rubin (center), Cranor: Free Networks now.

AS THE FATE OF NAPSTER IS DECIDED in court, the wider saga of distributed "peer-to-peer" networks is playing out elsewhere. New networks are springing up not only to help people avoid copyright laws, but also to enable them to share all types of digital information, free from censorship.

And such systems, which allow the sharing of information from many computers rather than central servers, are no longer created solely by solitary misfits. Two of the most prominent new networks, Publius and Freenet, have sharply contrasting backgrounds. Like Napster, Freenet is the brainchild of an individual: in this case, a 23-year-old Scottish programmer. Publius, on the other hand, was developed by researchers at AT&T Labs. Peer-to-peer is no longer a grassroots movement: It's becoming the province of

Anon.penet.fi stripped away identifying information and resent messages to their original destination. In 1995, after someone used Helsingus' brainchild to broadcast copyrighted

altered without the permission of the author. The system encrypts a document and divides it into fragments, or keys, that reside on multiple randomly selected servers. Though the document

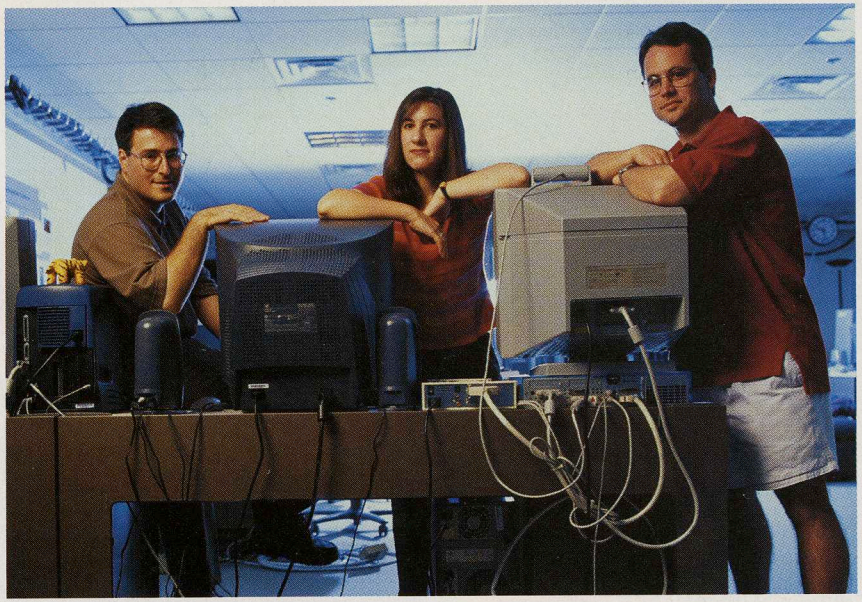
INTERNET_ANONYMITY

Speech without Accountability

New software makes it nearly impossible to remove illegal material from the Web—or to find out who put it there

SAN FRANCISCO—In the centuries-long struggle to decide what people may say without fear of prosecution, almost all the big decisions have been made by constitution writers, judges and politicians. When things work properly, these players balance one another out and change the limits of free speech only slowly and after much debate. Inventors have played an occasional starring role, too, Gutenberg being the archetype. But with the rise of the Internet, a certain class of inventors—computer scientists—has asserted its own special power to determine the boundaries of permissible speech. Unlike the leaders of governments, programmers release the new methods that they devise for sharing information globally, quickly and often with little thought to the consequences.

Consider Publius, a censor-resistant Web publishing system described in mid-August at a computer security conference in Denver. Engineers at the conference greeted the invention warmly, presenting to its creators—Marc E. Waldman, a Ph.D. student at **New York University**, and Aviel D. Rubin and Lorrie F. Cranor of **AT&T Labs-Research**—the award for best paper. Publius is indeed an impressive technical achievement: a tiny little program that, once widely installed, allows almost any computer user to publish a document on the Web in such a way that for all practical purposes it cannot be altered or removed without the author's



CENSOR BEATERS: Marc E. Waldman (*left*), Lorrie F. Cranor (*center*) and Aviel D. Rubin are the creators of Publius, an impressive tamperproof publishing system for the Web.

of Investigation would not comment on how it might track down those who use Publius to put illegal material on-line.

Publius thus appears to allow speech without accountability, and that is something fundamentally new. Deep Throat was anonymous, for example, but the *Washington Post* still had to defend its Watergate story in court. When antiabortionists made up a list of doctors who performed abortions and posted it on-line, striking through the names of those some of them start to act in response."

But is it an appropriate response for a small number of computer scientists to create software that subverts the efforts of governments, who must answer to citizens, and of companies, who must answer to both governments and customers? Publius has many obviously good uses, Rubin argues. "A whistle-blower could use it to expose illegal dumping by his employer. You could set up a Web site supporting a political candidate that your

Discussion

- Technology that can protect “good” speech also protects “bad” speech
- What if your dog does publish your secrets to the Internet and you can’t do anything about it?
- Is building a censorship-resistant publishing system irresponsible?
- If a tree falls in a forest and nobody hears it….

For further reading

- Publius chapter in Peer-to-Peer: Harnessing the Power of Disruptive Technologies edited by Andy Oram
- The Architecture of Robust Publishing Systems. ACM Transactions on Internet Technology 1(2):199-230 http://doi.acm.org/10.1145/502152.502154

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy