The DMCA & ACTA vs. Academic & Professional Research: How Misuse of this Intellectual Property Legislation Chills Research, Disclosure and Innovation

Tiffany Rad

Christopher Mooney

Tiffany Strauchs Rad, MA, MBA, JD

- tiffany@elcnetworks.com
- http://www.elcnetworks.com/
- President of ELCnetworks, LLC: Tech business consulting firm with a focus on information security, intellectual property, and entrepreneurship.
- Adjunct Professor in the computer science department, University of Southern Maine teaching computer law and information security
- Director/Founder of Reverse Space, a hackerspace in Northern Virginia
- I'm a lawyer, but not your lawyer

Christopher Mooney

- https://chris.dod.net/
- chris@dod.net
- @godsflaw on Twitter
- I have a computer science degree from the University of Southern Maine
- Software engineer at http://craigslist.org/
  - This talk may not reflect craigslist’s views
- Current acting executive director of Project DoD, a 501 (c)(3) nonprofit: http://home.dod.net/
- If you were at DEFCON last year, I presented Subverting the World of Warcraft API

DMCA and ACTA

- The Digital Millennium Copyright Act (DMCA) is increasingly being used in ways that chill free speech, disclosure of security vulnerabilities and innovative research.

- If the ACTA (Anti-Counterfeiting Trade Agreement) is passed, many countries will experience similar chilling effects as we have in the United States.

The Unfair Corporate Advantage

- You run a software company.
- You and a competitor are about to launch similar products in the marketplace.
- If your company is quick, you will have the advantage of being first to market.
- Your ISP is flooded with DMCA take-down notices regarding your new software's source code.

- Result: Most, if not all, of your company's site is removed by your ISP. The day planned for launch, you have no online presence. You miss being first to market.

Silencing Discussion of Security Vulnerabilities

- You are a security researcher.
- You are _$B!G_ and are racing another researcher with a similar vulnerability disclosure. You are all about the 0-day, to slow down the other researcher, you file multiple DMCA take down notices to his ISP.
- You decide to let the ISP sort through whether or not the take down notices are legitimate.

- Result: His blog, social networking accounts and his company's site are down. You post your 0-day.

Chilling Online Critique

- You have been injured by the medical techniques implemented by a physician.
- You would like for other doctors and patients to know that something went wrong with your treatment.
- You take short snippets of the doctor's books using Fair Use techniques.

- Result: Your blog--and all critique mentioning this doctor's name--is offline because your ISP has received multiple and repetitive DMCA take down notices. No one can discuss online anything negative about this doctor or his techniques.

Are these situations fact or fiction?

DMCA

- Prohibits the dissemination, production and creation of technologies that circumvent technological measures implemented to protect copyrighted works. Accessing works that are protected by (DRM) or anti-circumvention measures, such as encryption, is a violation of the DMCA.

- Signed into law by President Clinton in 1998. It amended the Title 17 of the U.S. Code for copyright while limited liability of ISPs for copyright infringement of their users

37% of DMCA Takedown Notices Google Receives are Invalid

- Google made a submission to the Telecommunications Carriers Forum in New Zealand critiquing the draft code of practice for ISPs in relation to section 92A of the Copyright Act.

- 57% of the invalid notices were sent by business targeting competitors and over one third (37%) of notices were not valid copyright claims.

- Reference: "Google Submission Hammers Section 92A," New Zealand PC World:

  http://pcworld.co.nz/pcworld/pcw.nsf/feature/93FEDCEF6636CF90CC25757A0072B4B7

Anti-Counterfeit Trade Agreement (ACTA)

- An international intellectual property enforcement organization outside of any single country's jurisdiction. The new legal framework or governing body, so far, outside of WIPO (World Intellectual Property Organization), WTO (World Trade Organization) and the U.N.

- Addresses "increasing" international IP infringement regarding counterfeit goods (purses, watches), generic medicines, and online copyright infringement such as music and software.

- Increased authority for searches and seizure at boarders.

- Increased cooperation between signatory country law enforcement agencies

Proposed Parties to the ACTA

- Japan, U.S., European Union, Switzerland, Australia, Mexico, Morocco, New Zealand, Republic of Korea, Singapore
- There is a recent draft prepared and released for the public April 10, 2010
- If the ACTA is passed, many countries will experience similar chilling effects as we have in the United States
- http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf

Notes about the talk

- Types of ISPs this talk is about
  - not last-mile providers
- Internet Service Providers
  - Hosting providers
  - Facebook
  - Twitter
- All questions are rhetorical

Why is this talk relevant after more than ten years of the DMCA?

- DMCA abuse is increasing
- C-32 (Canada)
- Digital Economy Bill (UK)
- ACTA (International)

Who is Project DoD (dod.net)?

- All volunteer run 501(c)(3) charitable nonprofit
  - Looks like an open source project
  - dod.net is funded by donations
- dod.net's biggest project is hosting
  - started hosting the needy
  - gravitated towards censorship resistant hosting
- Now developing a censorship resistant jurisdiction hopping infrastructure to remedy some of the problems in this talk.

Project DoD v. Federici

- Relevance of DoD v Federici
- We will address DMCA takedown abuses; this case touches on all of them.
- This case is perhaps one of the more concerning chilling effects of DMCA-style takedown provisions.

Two Questions

If our medicine is based on science, what does it mean for society if the peer-review process is censored?

If open discussion and responsible disclosure of security vulnerabilities is censored, how safe is our society?

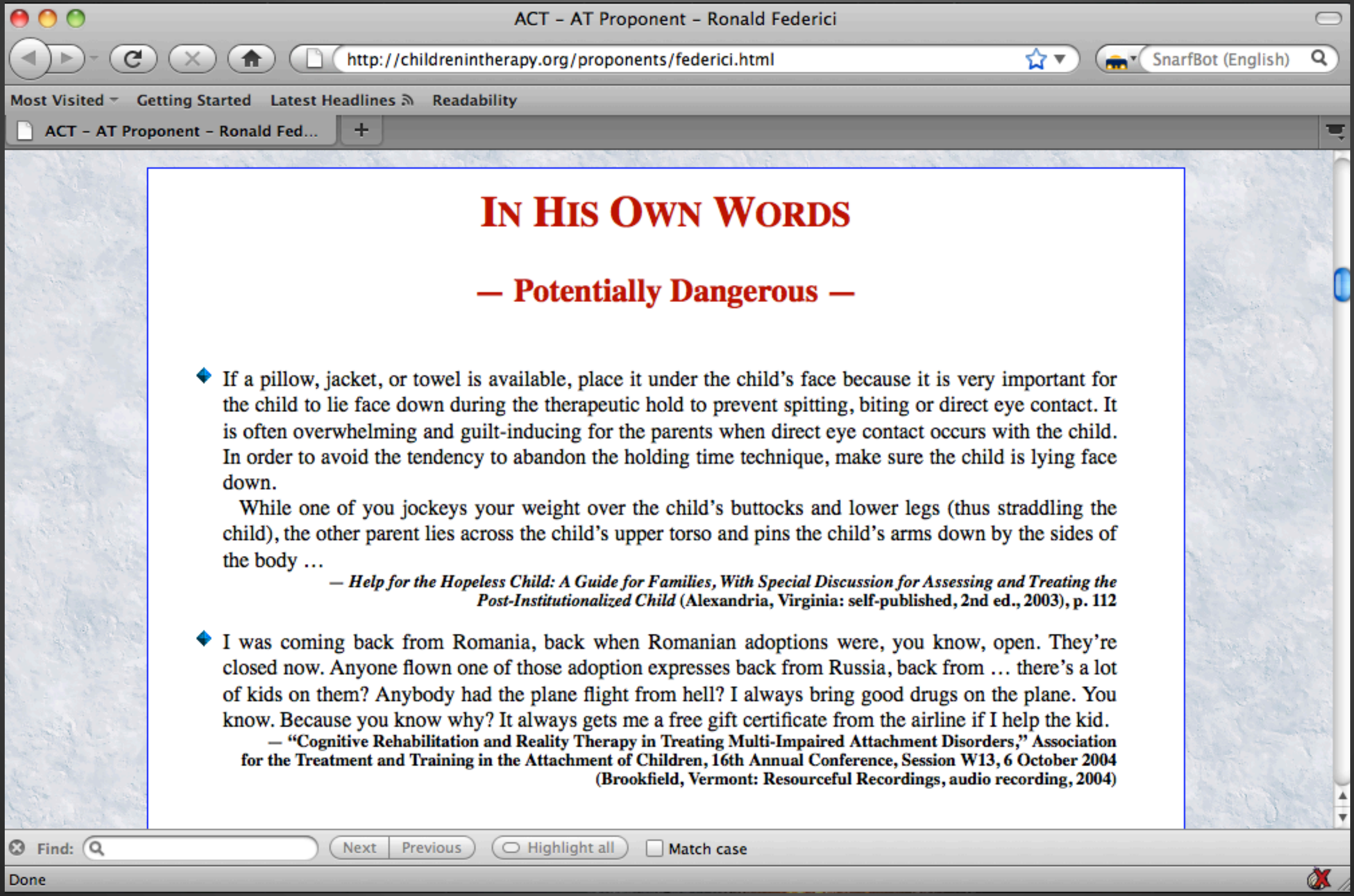
Background

- Federici and attachment therapy
- He treats Reactive Attachment Disorder
  - Restrain child to break them down
  - Reform the bond
- Advocates for Children in Therapy (ACT) is trying to stop the practice of attachment therapy
- "Law and Order" episode is closely based on the facts, but names were changed

More Background

- Federici legally engaged ACT for libel and slander
- ACT restructured their page to site material and allow people to draw their own conclusions.
- Truth is protection against libel and slander?

ACT Quotes Page


ACT – AT Proponent – Ronald Federici
http://childrenintherapy.org/proponents/federici.html
SnarfBot (English)
Most Visited
Getting Started
Latest Headlines
Readability
ACT – AT Proponent – Ronald Fed...
+
Find:
Next
Previous
Highlight all
Match case
Done

IN HIS OWN WORDS

— Potentially Dangerous —

- If a pillow, jacket, or towel is available, place it under the child's face because it is very important for the child to lie face down during the therapeutic hold to prevent spitting, biting or direct eye contact. It is often overwhelming and guilt-inducing for the parents when direct eye contact occurs with the child. In order to avoid the tendency to abandon the holding time technique, make sure the child is lying face down.

  While one of you jockeys your weight over the child's buttocks and lower legs (thus straddling the child), the other parent lies across the child's upper torso and pins the child's arms down by the sides of the body …

  — *Help for the Hopeless Child: A Guide for Families, With Special Discussion for Assessing and Treating the Post-Institutionalized Child* (Alexandria, Virginia: self-published, 2nd ed., 2003), p. 112

- I was coming back from Romania, back when Romanian adoptions were, you know, open. They're closed now. Anyone flown one of those adoption expresses back from Russia, back from … there's a lot of kids on them? Anybody had the plane flight from hell? I always bring good drugs on the plane. You know. Because you know why? It always gets me a free gift certificate from the airline if I help the kid.

  — "Cognitive Rehabilitation and Reality Therapy in Treating Multi-Impaired Attachment Disorders," Association for the Treatment and Training in the Attachment of Children, 16th Annual Conference, Session W13, 6 October 2004 (Brookfield, Vermont: Resourceful Recordings, audio recording, 2004)

Enter, the DMCA

- Federici finds out about DMCA takedown notices
- Federici files notice with mom-and-pop hosting shop
  - ACT is kicked off no counter-notice
  - ACT moves to Network Solutions
- Federici files takedown notices with Network Solutions
  - ACT is kicked off with no counter-notice

ACT Finds Project DoD

1 Federici files takedown notices requesting the entire site come down.

2 We allow a counter notice

3 Content down for 10 business days

4 Content comes back up

5 Our upstream provider is harassed

6 Electronic Frontier Foundation (EFF) steps in to back our provider

7 Federici has other doctors send the same takedown notice for similar pages for three months. Portions of ACT's site are down for that time

8 Six months goes by with no word

9 Federici has attorney file takedown notice for the same, exact, content again.

10 We use provision 512(f) to stop Federici.

11 Arguments are made and Maine dismisses case for lack of personal jurisdiction.

12 Federici files another DMCA takedown notice, the third one, for the same content.

13 We are left with no choice but to pursue Federici in Virginia

Common Abuses for DMCA Takedown Provisions

- Fair Use is not a magic bullet
- Statutory waiting period, or statutory denial of service attack
- Backdoor takedowns
- Endless chain attack
- Leveraging a 512(g) counter notice to discover one's identity
- ISP liability

Fair Use is Not a Magic Bullet

- Provision 512(f)
- As of 2008 we have Lenz v. Universal
- Fair use hard to determine
- Therefore fair use is hard to use as a defense against DMCA takedown abuse
- In our experience, this makes 512(f) very hard to use.
- Jurisdictional problem with 512(f)

Examples of takedowns without considering Fair Use

- In 2005 walmart-foundation.org and 700-club.org
  - Subversive media class at Carnegie Mellon University
  - Up for about two weeks before they were taken down
  - Both users struggled with choice to file a counter-notice
- Project DoD v. Federici even after Lenz v. Universal

Statutory Waiting Period, or Statutory Denial of Service Attack

- Upon receipt of a counter notice, in order for the ISP to maintain its safe harbor, the content must stay down for a statutorily required 10 business days.

Example of waiting period abuse

- Federici figured out the content would be down for ten days
- Six of Fererici's colleagues sent takedown notices
- Parts of the site were down for months

Backdoor Takedowns

- Classifications of ISPs
- ISPs register a designated agent with the copyright office
- There is no specific wording that prevents someone from sending notices to upstream providers
- De facto process is to look up the IP address in ARIN
- Dangers of having a handful of providers make content decisions
- Virtual Private Server hosting could be problematic

Examples of backdoor takedowns

- We've been hosting users for twelve years and have too many cases to recount here
- It is the most common reason over the past twelve years that we have switched providers
- One case that stands out is hackblock.org
  - above.net
  - takedown notice for the original takedown notice
  - above.net threatened to shut us off, and all of our users
  - We had a statutory right to arbitrate this second notice
- Today we have a more functional relationship with our upstream providers
  - Project DoD v Federici
  - Silicon Valley Web Host (SVWH) maintained common carrier status
  - EFF stepped in to backup our upstream provider

Endless Chain Attack

- After the full process of notice / counter notice, rinse and repeat
- There is no specific wording in the DMCA that stops repeat notices
- There may be an implication from the 10 day waiting period
- It takes a lot of time to verify that new notices are indeed new

Examples of the Endless Chain Attack

- Project DoD v. Federici
- It was this abuse of process that prompted us to take Federici to court
- On our third notice from Federici
- Still very time consuming

Leveraging a 512(g) counter notice to discover one's identity

- Counter notices require personally identifying information
  - Note that takedown notices do not require this (agent wording)
- Section 512(h) requires a court order to release identity

Example of this abuse

- Separate case on dod.net where Federici sent a takedown notice for stopchildtorture.org
- NBC video that showed a link between facedown takedown and Federici's holding techniques
- Content went down and the user did not want to compromise their identity

ISP liability is a significant failure of the DMCA

- Alleged rights holder and alleged infringe
- Passionate arguments should be made by those most directly affected by the content
- The statute ties ISP's liability to content as a contributory infringer
- ISPs are motivated by profit and an industry with thin margins
  - De facto state of censorship
- One can switch from independent providers to an ISP like dod.net
  - One cannot do this on Twitter or Facebook
  - The future will get much worse

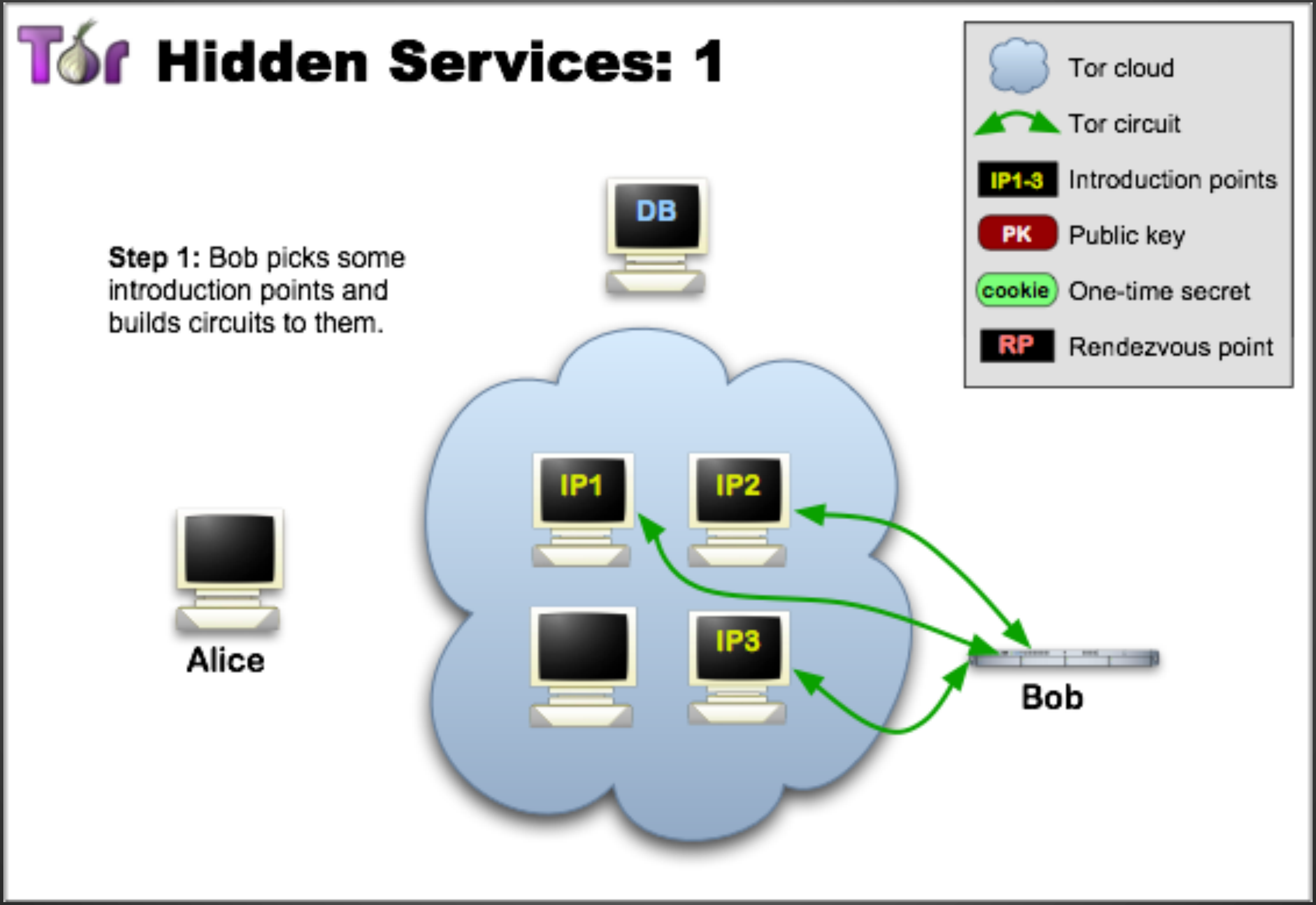
Examples censorship because of ISP liability

- WordPress
- GoDaddy
- Network Solutions
- A bunch of smaller providers

Can technology fix these censorship problems?

- There might be a couple technical solutions
- Quick Overview Tor Hidden Service
  - Thank you Tor folks
  - Assume knowledge of normal Tor circuit
- Jurisdiction hopping solutions
- Direct action

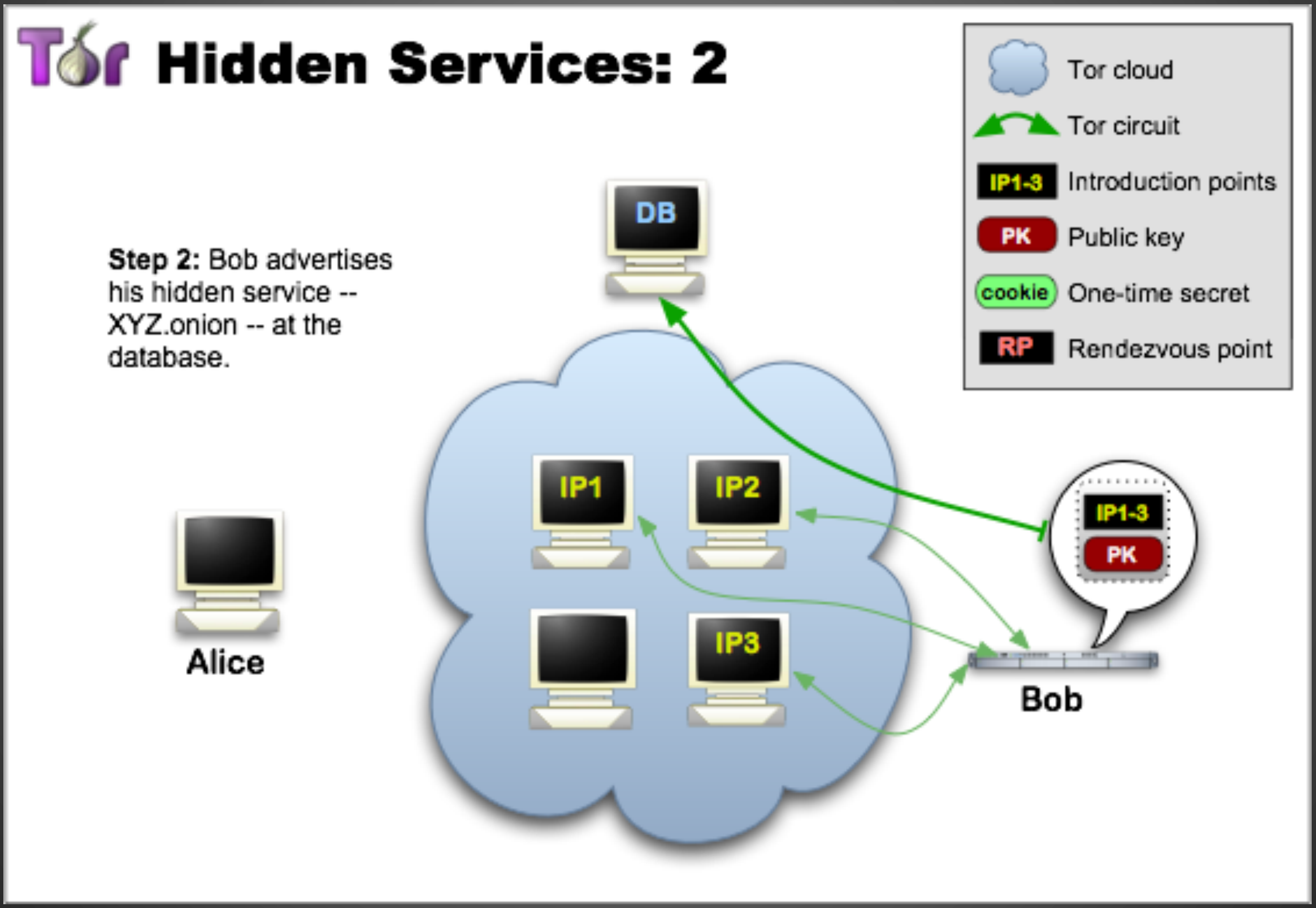
ISP picks introduction points



Tor Hidden Services: 1

Step 1: Bob picks some introduction points and builds circuits to them.

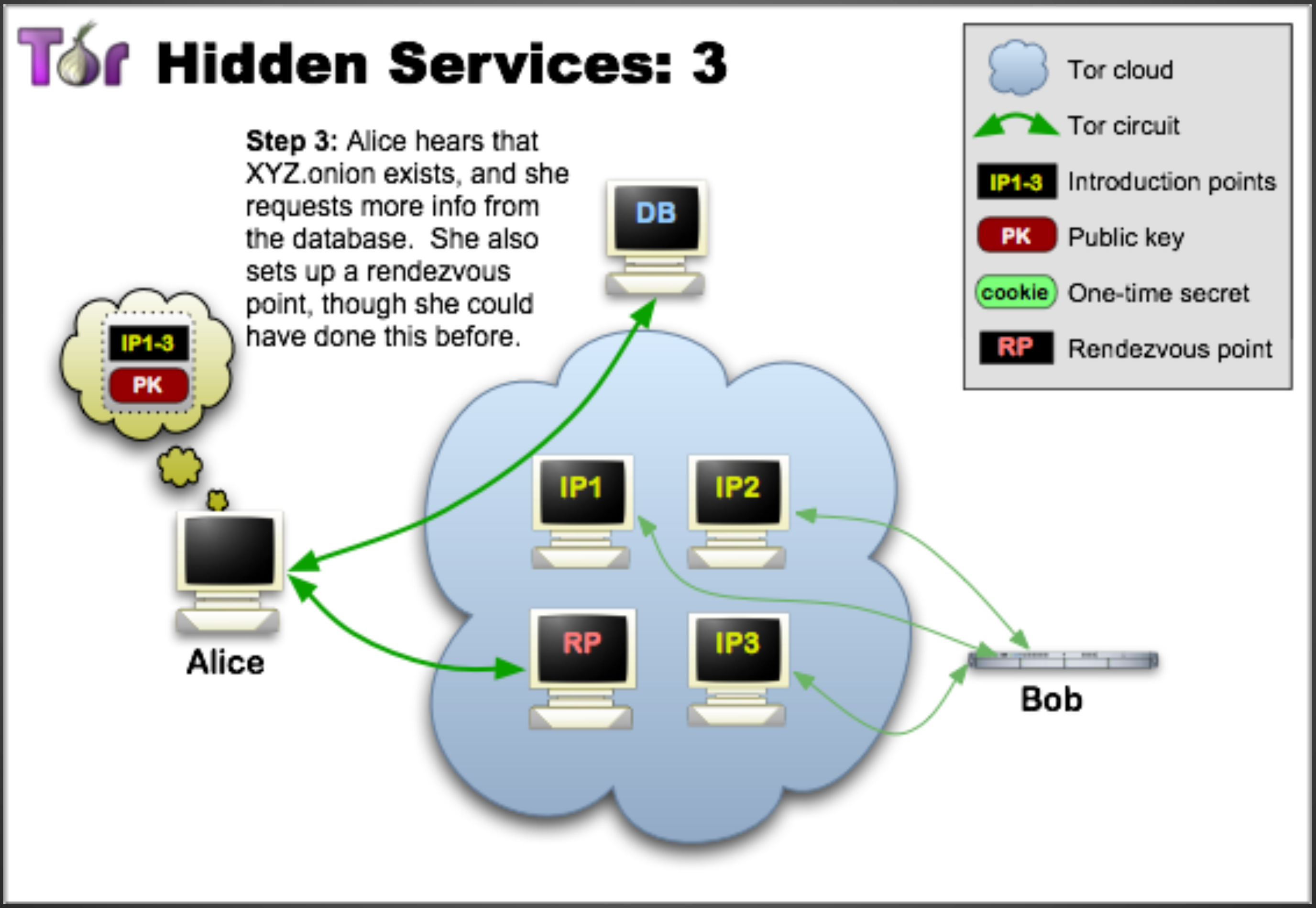
ISP lists itself with the service directory



Tor Hidden Services: 2

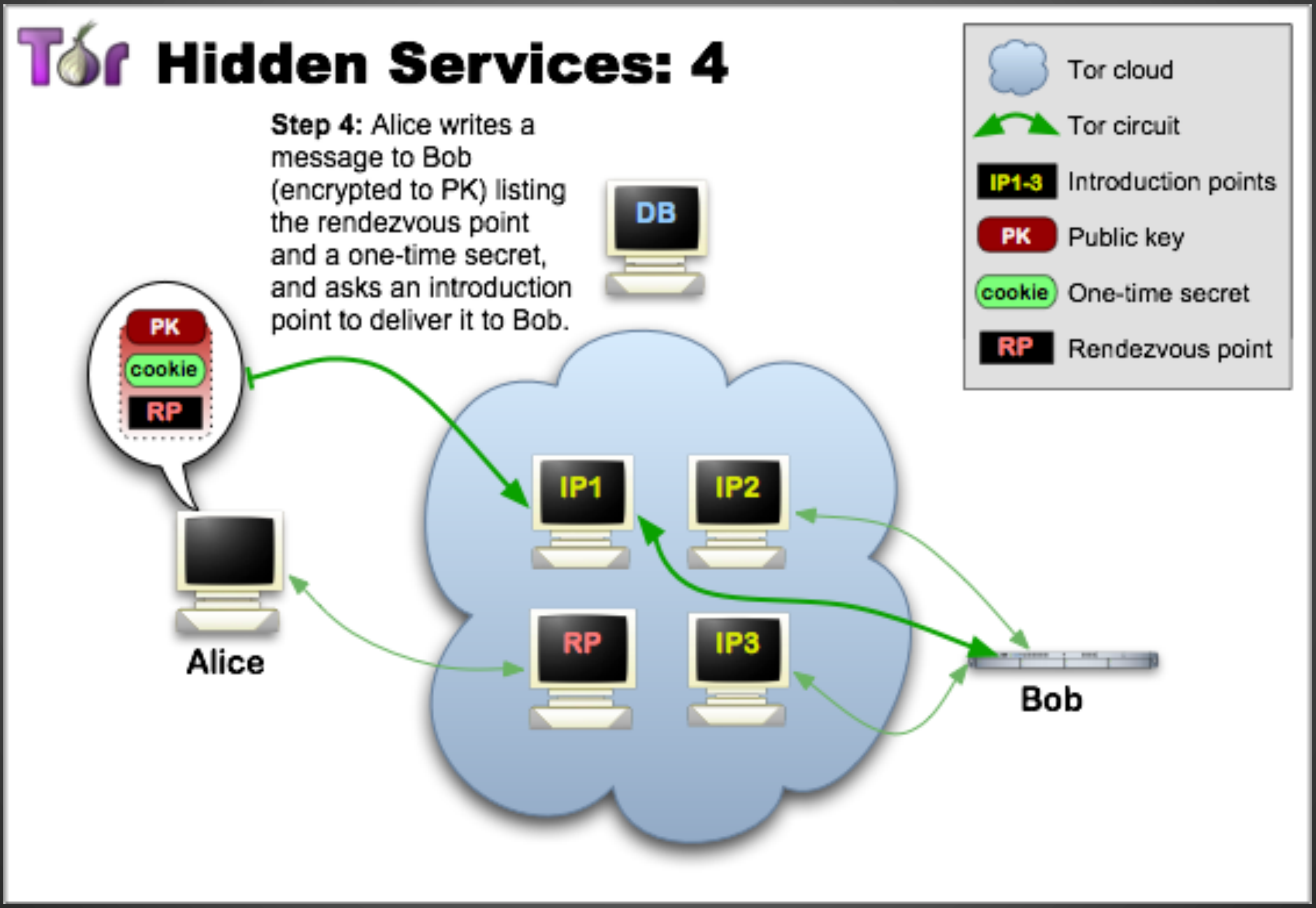
Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.

The user looks up that resource and picks a rendezvous point



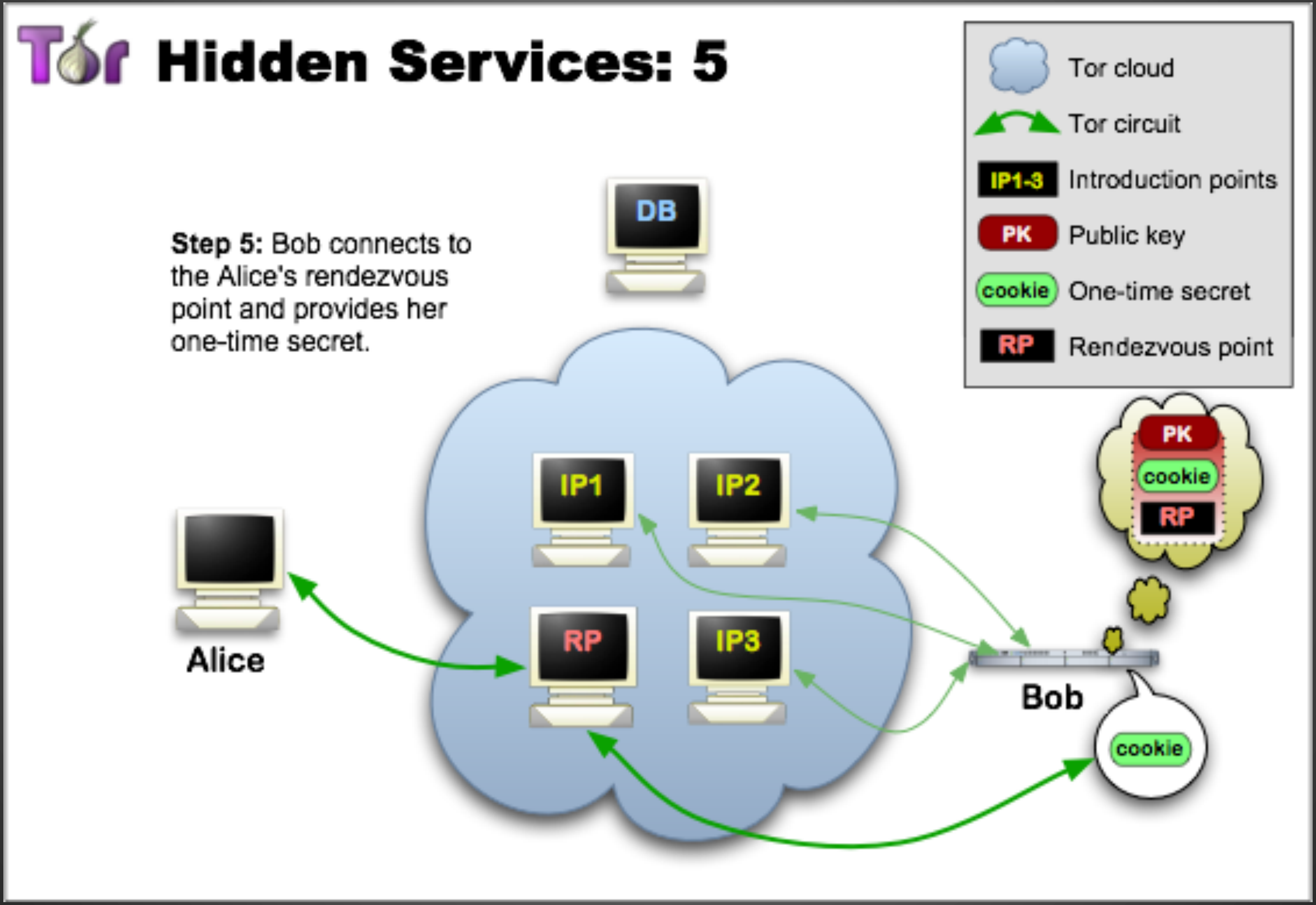
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

The user contacts the ISP through the introduction point



Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

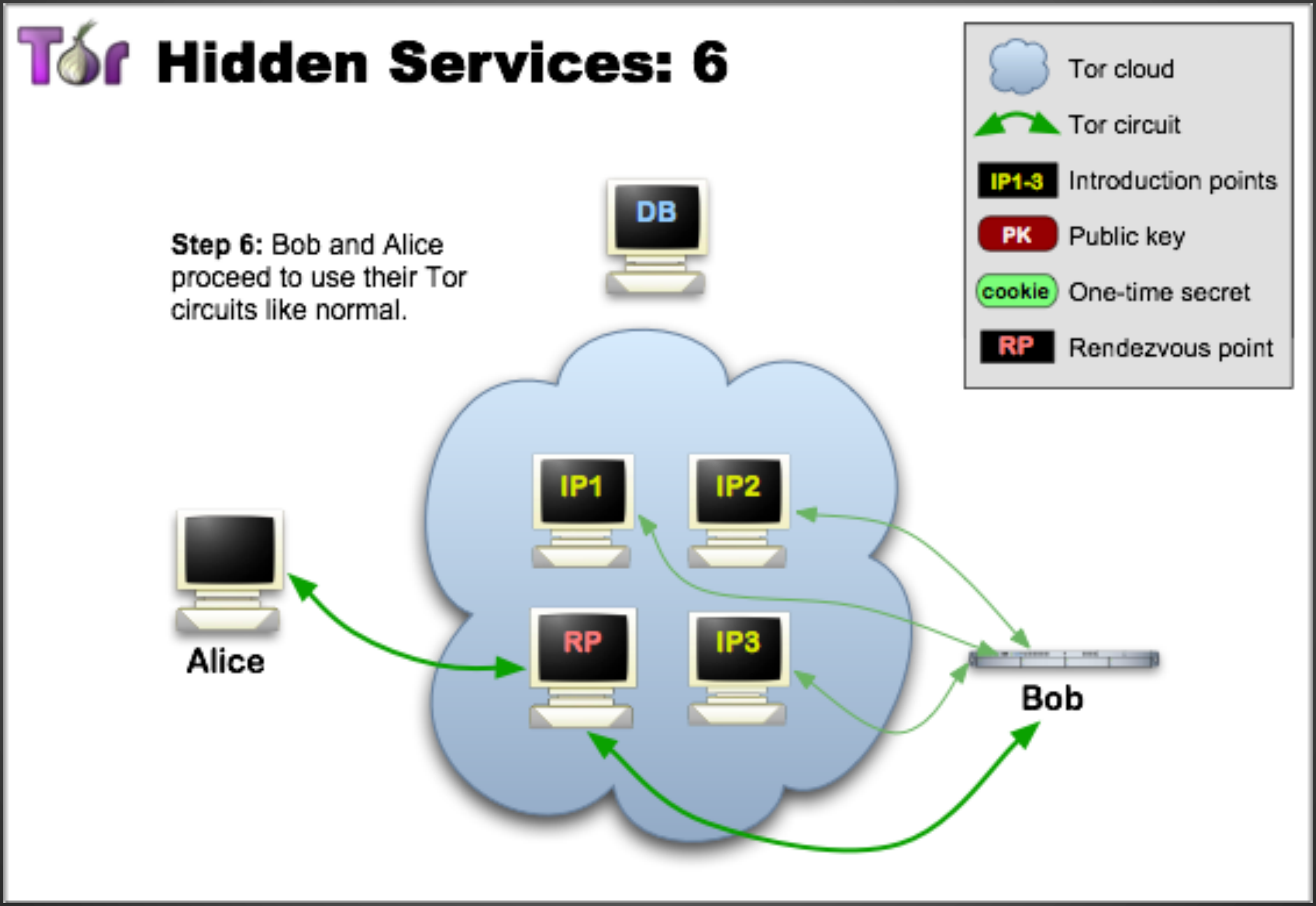
The ISP meets the user at the rendezvous point



Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.

They communicate over an encrypted channel



Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.

The spectrum of users

- There is a latency hit for traversing the Tor network on ISP and user side.
- The directory lookup and obscure identifier are unfortunate.
  - Artifact of Zooko's conjecture
    - human-meaningful (memorable)
    - secure (secure mapping)
    - decentralized (no name authority)
- There is a more user friendly interface to it called tor2web.
  - http://tor2web.com/
- tor2web can be leveraged to solve the name problem with URL redirects.
  - But this means we now have a central name authority
  - Trade-off decentralized for human-meaningful

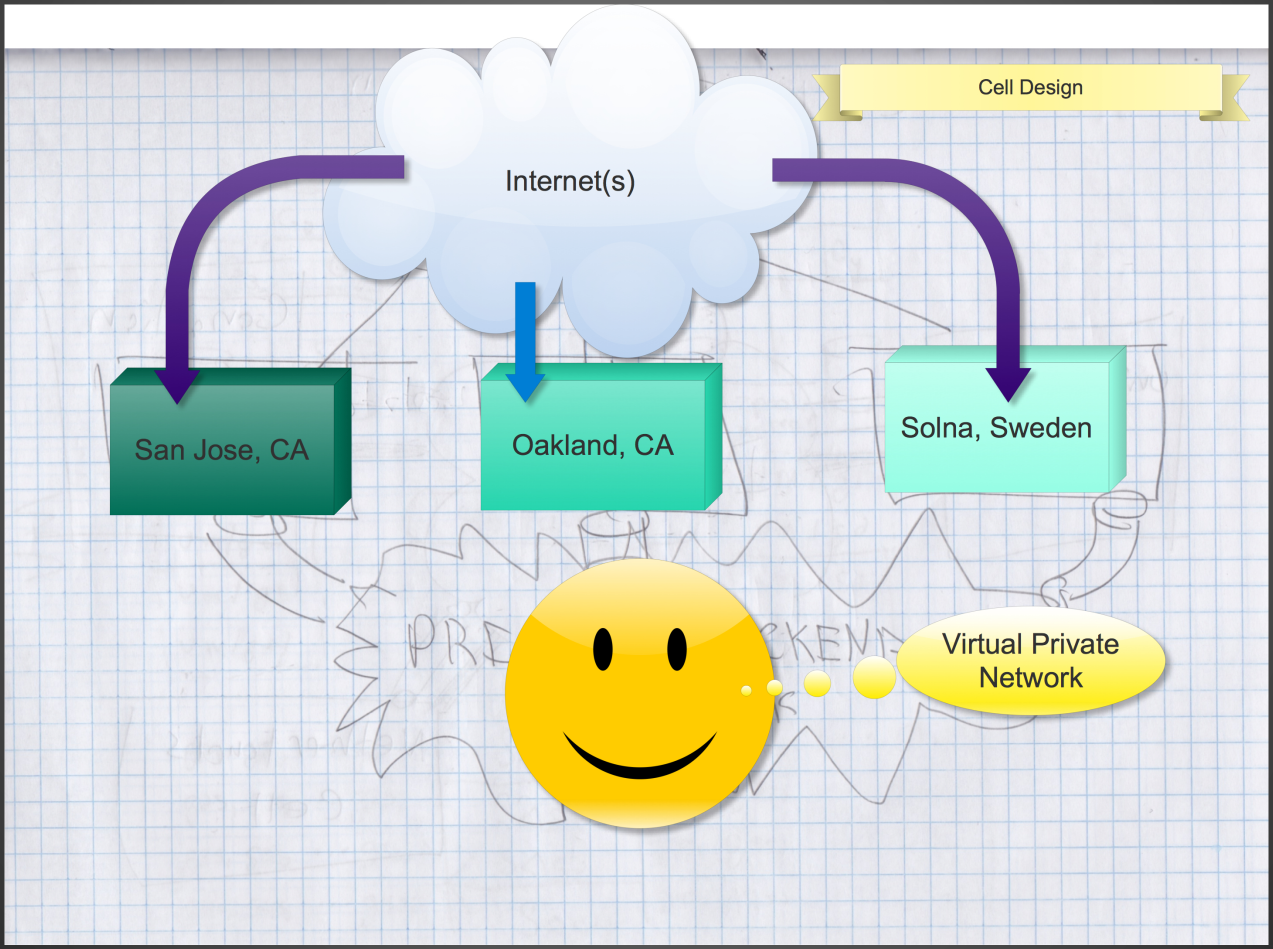
Jurisdiction Hopping

- How does jurisdiction hopping work?
- Haven Co.

What Project DoD is working on

- We are pulling together a bunch of tools and developing a distributed infrastructure.
  - We have nodes in San Jose, Oakland, and Sweden
- Our hopes are that we can gain censorship resistance through jurisdiction hopping.
- This is a stop-gap solution until there is wide-spread adoption of a protocol (like Tor)
  - "cell" as in guerrilla

Overview of a “cell”



Cell Design

Internet(s)

San Jose, CA

Oakland, CA

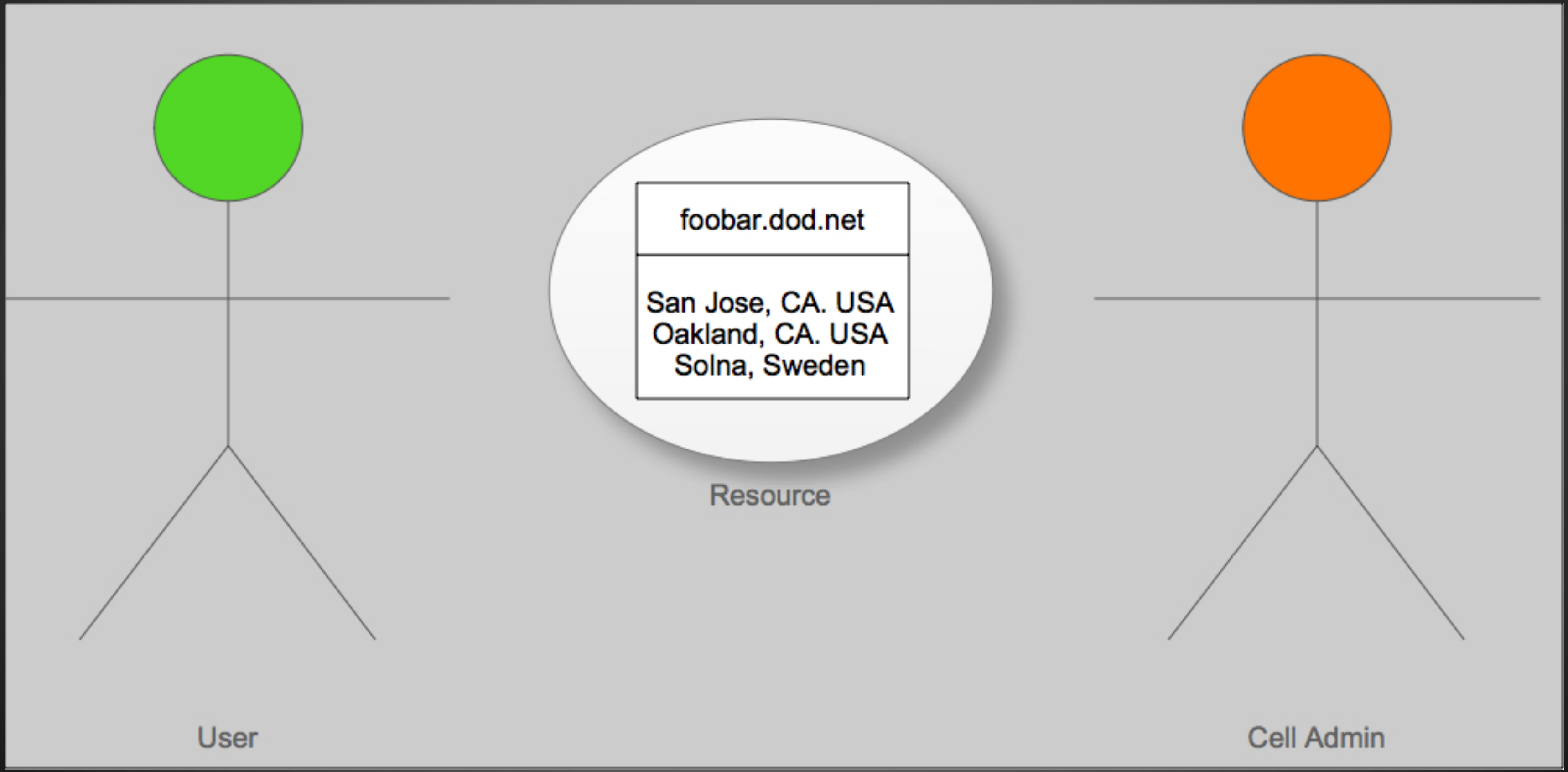
Solna, Sweden

Virtual Private Network

Distribution of Responsibility and Isolation of Control

- Admins should have control over their cell's resources.
- Users should have control over where a resource is located.

Resource Jurisdictions



foobar.dod.net

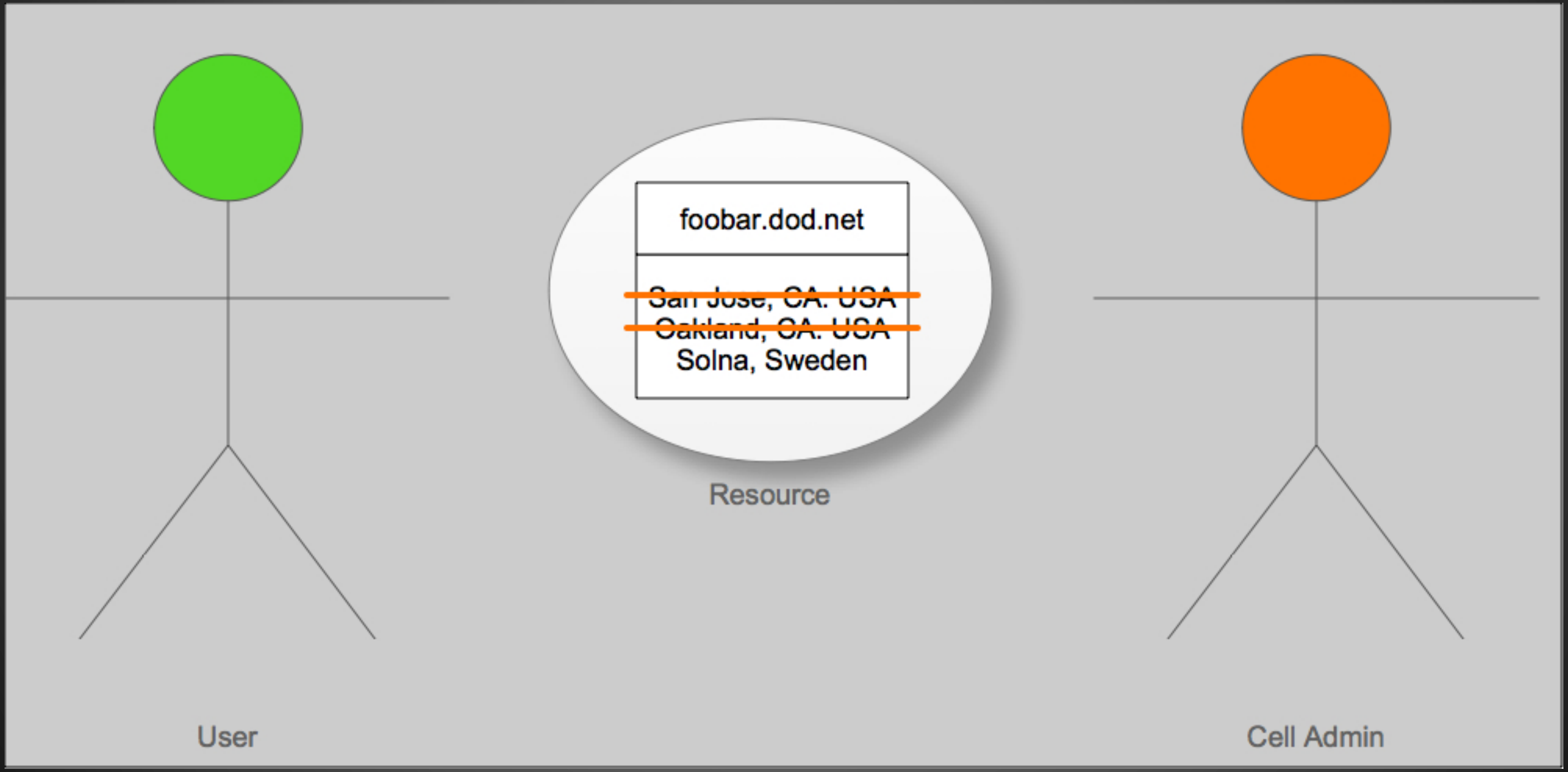
San Jose, CA. USA
Oakland, CA. USA
Solna, Sweden

Resource

User

Cell Admin

Admin removes resource from nodes



foobar.dod.net

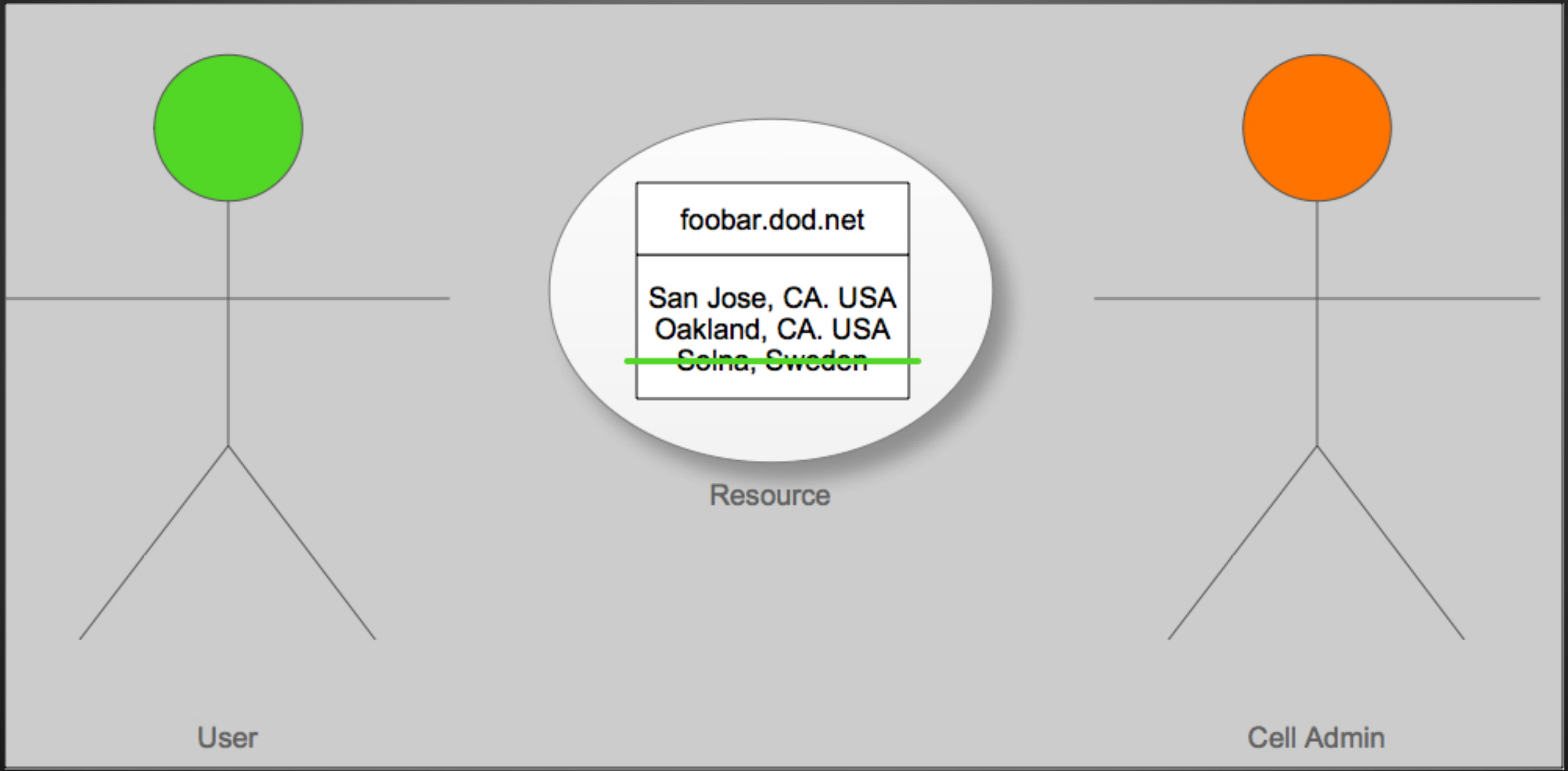
~~San Jose, CA. USA~~
~~Oakland, CA. USA~~
Solna, Sweden

Resource

User

Cell Admin

User removes access to resource in certain jurisdictions



Redundancy of Data

- Data needs to be in more than one jurisdiction at a time.

A Resource Should have Jurisdictional Resilience

- Resources should enjoy jurisdictional diversity
- The individuals and organizations that control those resources should also be diverse

DMCA Abuse Thought Experiment

- Major DMCA-takedown protocol flaws outlined above.
  - Guilty until proven innocent 10-day DoS Attack
  - backdoor takedowns
  - the endless chain attack
  - ISP liability

Rhetorical Questions

- What if we treat the failings of the DMCA takedown provisions as protocol failings?

- What if we treat law makers like software vendors?

- What if proof-of-concept code could be used to highlight DMCA protocol flaws?

Responsible Disclosure

1. Vendor releases buggy software.
2. Security research finds theoretical vulnerability and informs the vendor.
3. Vendor chooses not to fix bug.
4. Researcher releases theoretical white paper about the vulnerability.
5. Vendor still does nothing, arguing that the bug is pure theory.
6. Researcher writes proof-of-concept code to exploit bug.
7. Vendor must fix bug.

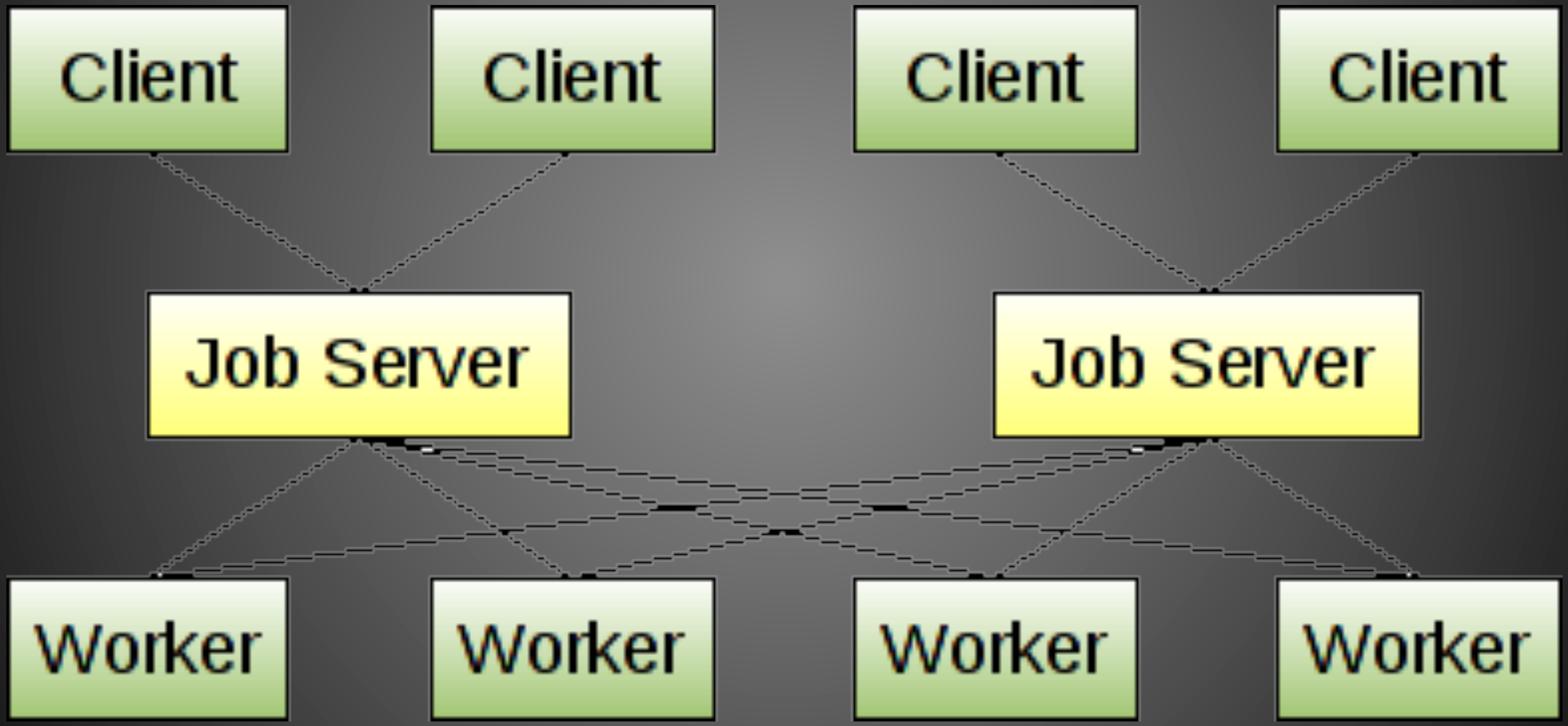
Theoretical Attack

- Let us imagine what happens when we amplify the attacks in Project DoD v. Federici
- Posit an anonymous malicious actor named Mallory.
- Design (or use) a bot network of nodes that can send well-crafted DMCA takedown notices, and follow up notices, to multiple ISPs against multiple users.

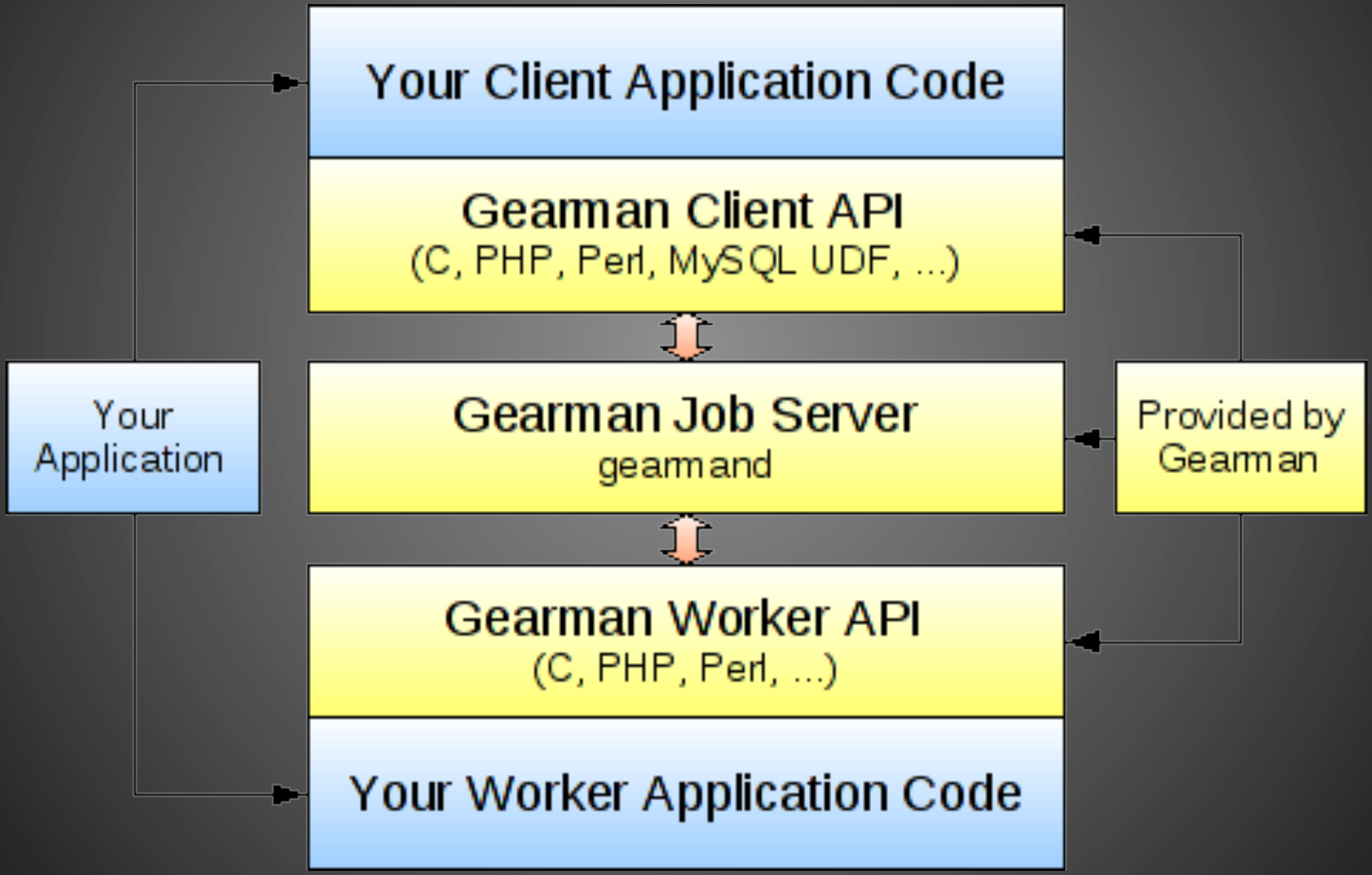
How would one design this proof-of-concept code?

- Requirements
  - Mallory's identity stays hidden.
  - The nodes that do the sending cannot be traced back to their controllers.
  - The nodes do need to be exposed.
- The abusive takedown notice must looks like a legit notice.
  - Random legit looking letter head (chillingeffects.org).
  - anonymous contact information like phone and email (VOIP, pre-paid, Tor).
  - Contact for counter notice (access anon email).
- Notices are sent to search engines, and first-order ISP.
  - Follow up notices are sent when needed.
  - If content is still up at the end state or no response is taken, then
    - rinse and repeat to the nth-order ISP.

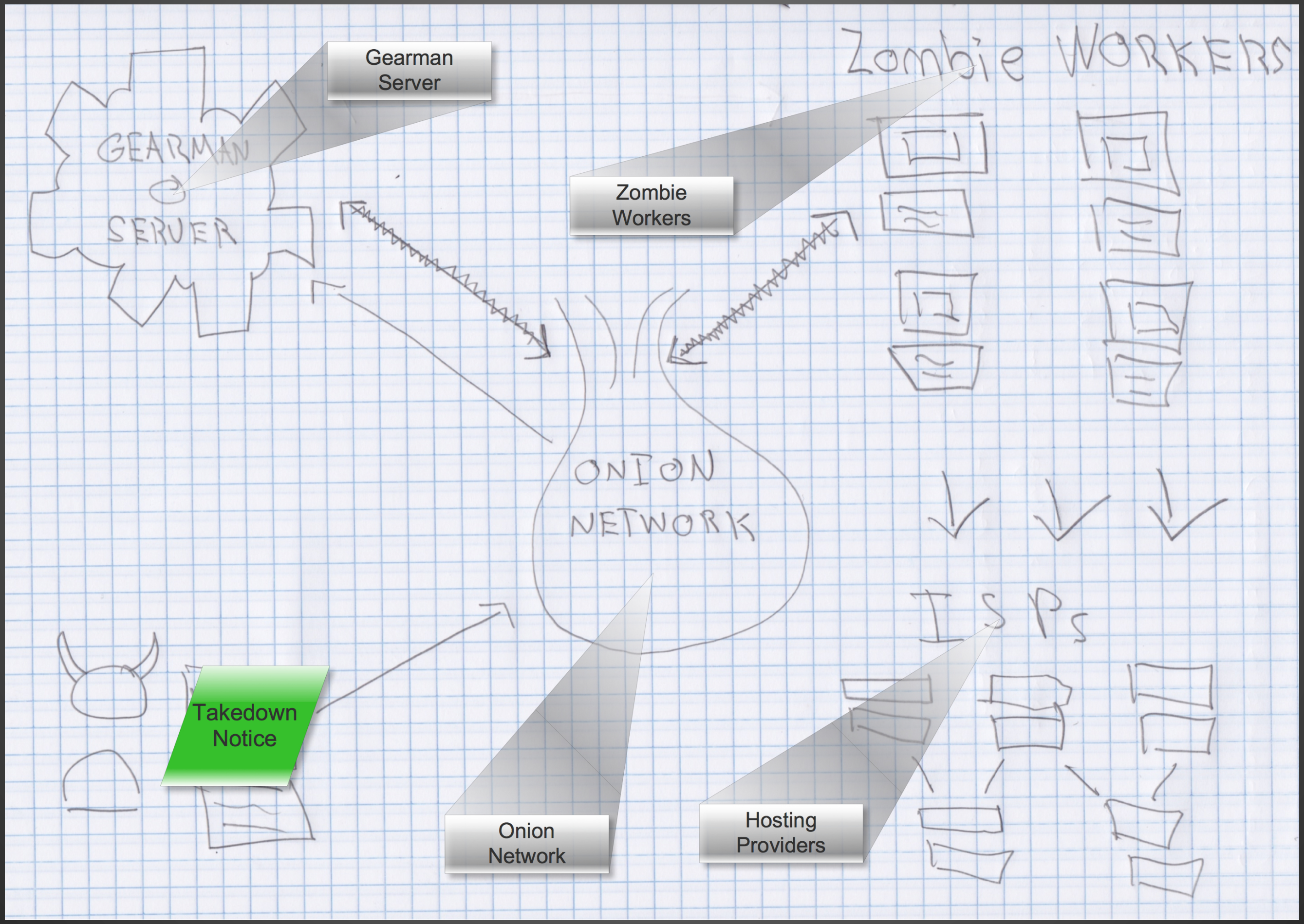
Gearman


Client
Client
Client
Client
Job Server
Job Server
Worker
Worker
Worker
Worker

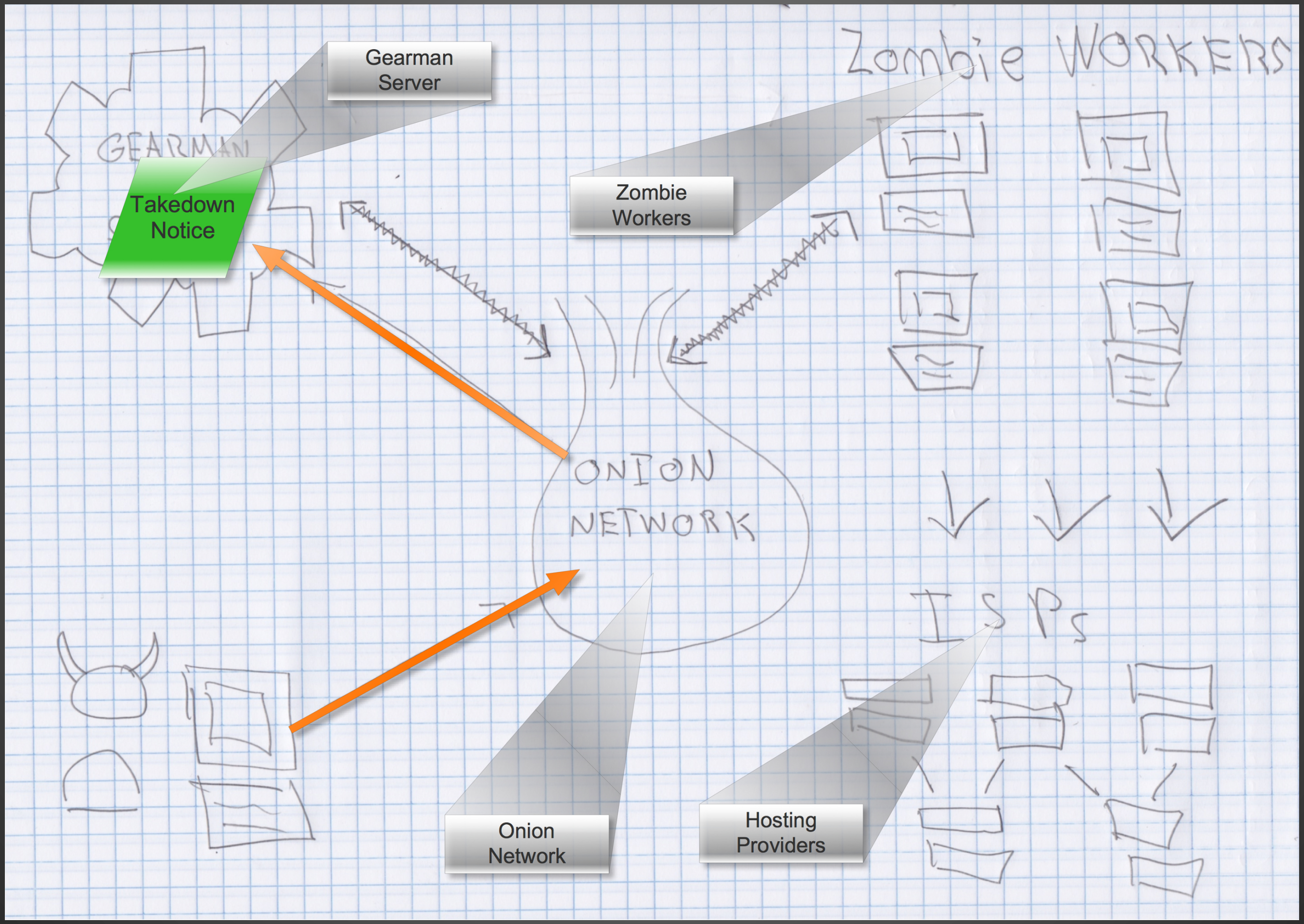
Gearman Stack



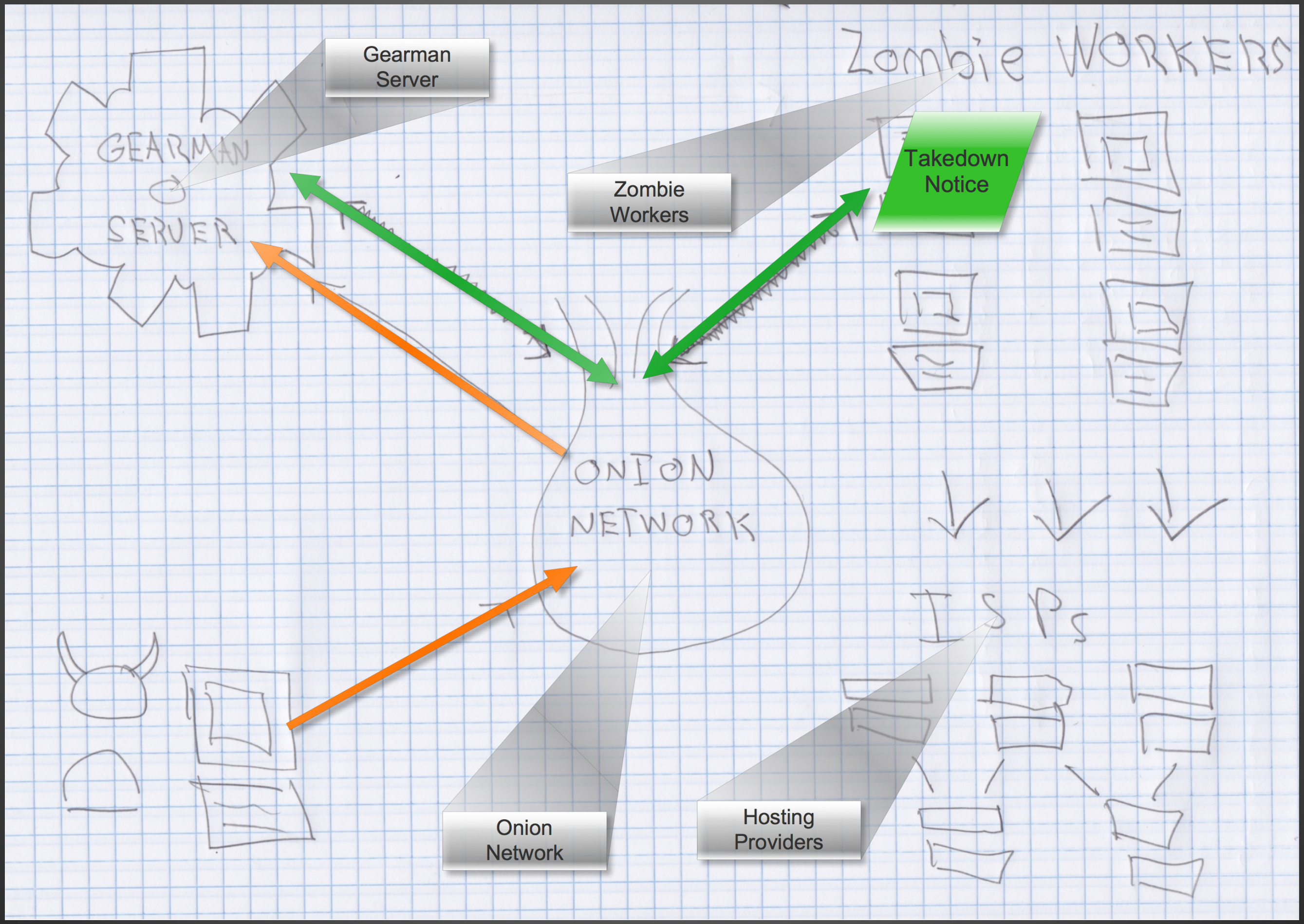
Basic Network



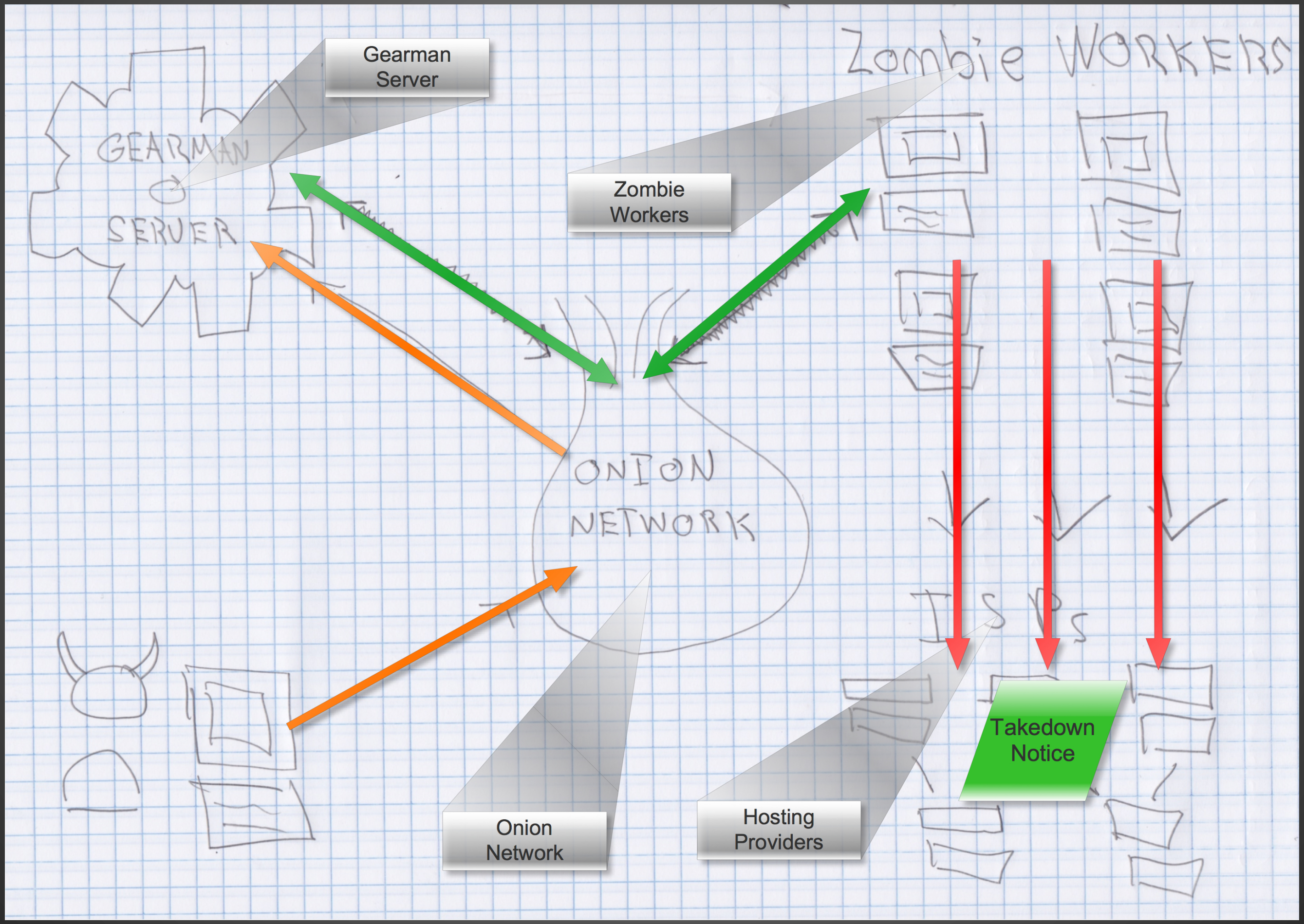
Takedown notice sent from client to Gearman server



Takedown notice moves to worker



Takedown notice goes off to nth-order ISPs



End Results

- Service providers may follow counter-notice provisions.
  - But then there is the 10-day DoS.
  - Abuse takes into account backdooring and chaining attacks.
- Volume is great enough for ISPs to stop compliance with the DMCA.
- Law becomes unenforceable and must be changed.

How does one fix DMCA-style takedown provisions

- Remove the 10-day DoS
- Disallow the chaining attack by changing the statute to not allow notices for the same content more than once.
- Change wording of the statute to require action ONLY by the designated agent at the service leaf nodes.
- All above solutions still leave these problems.
  - ISPs shut users off because threats of liability, even with safe-harbor, are scary.
  - ISPs shut users off because the counter-notice process takes too much time under abuse.
  - We're right back at the biggest problem: ISP liability as a contributory infringer.
- So Remove ISP liability and thus the De facto state of censorship

What would this future look like?

- It would look a lot like our not-so-distant past.
- People would be innocent until proven guilty.
- Content would have to come down through a court order.

Conclusions

- Clearly DMCA-style takedown laws are flawed.
- We've talked about technical solutions to resist this form of censorship.
  - Tor hidden services
  - Jurisdiction hopping
  - Change through direct action
- We've talked about how to change takedown statutes to stop these types of abuses.

Questions?

Paper: http://dod.net/dmca_paper.pdf

Slides: http://dod.net/dmca_slides.pdf