The challenges of online protest

Joseph Bonneau

jcb82@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Festival of Ideas

Cambridge, UK

October 23, 2010

The dream of online protest

Election protests, Iran 2009

The dream of online protest

Nestlé environmental protests, 2009

The bitter reality

Carl Campbell OWNER OF **FACEBOOK** HAS CONFIRMED THAT THEY WILL SEND $1 DOLLAR TO THE RESCUE FUND FOR THE **HAITI** EARTHQUAKE DISASTER FOR EVERY TIME THIS IS CUT AND PASTED AS A STATUS. YOU ONLY HAVE TO LEAVE IT UP FOR 1 HOUR. LET'S ALL DO IT TO SUPPORT THANKS!!!!!!

5 seconds ago

Kris Van Donkersgoed THE OWNER OF **FACEBOOK** HAS CONFIRMED THAT THEY WILL SEND $1 DOLLAR TO THE RESCUE FUND FOR THE **HAITI** EARTHQUAKE DISASTER FOR EVERY TIME THIS IS CUT AND PASTED AS A STATUS. YOU ONLY HAVE TO LEAVE IT UP FOR 1 HOUR. LET'S ALL DO IT TO SUPPORT THANKS!

12 seconds ago

SengHock Lee ... the site. This will be done in remembrance of all the lives lost in **Haiti**'s Earthquake thispast week. If you agree please copy. http://apps.**facebook**.com/st_lfdtwo_b/

16 seconds ago

Karen Gallagher THE OWNER OF **FACEBOOK** HAS CONFIRMED THAT THEY WILL SEND $1 TO THE RESCUE FUND FOR THE **HAITI** EARTHQUAKE DISASTER FOR EVERY TIME THIS IS CUT AND PASTED AS A STATUS. YOU ONLY HAVE TO LEAVE IT UP FOR 1 HOUR. LET'S ALL DO IT TO SUPPORT **HAITI**. THANKS!

17 seconds ago

Vera Streicher THE OWNER OF **FACEBOOK** HAS CONFIRMED THAT THEY WILL SEND $1 DOLLAR TO THE RESCUE FUND FOR THE **HAITI** EARTHQUAKE DISASTER FOR EVERY TIME THIS IS CUT AND PASTED AS A STATUS. YOU ONLY HAVE TO LEAVE IT UP FOR 1 HOUR. LET'S ALL DO IT TO SUPPORT THANKS!!!!!

8 seconds ago

The bitter reality

causes Home Find Causes Best Of Account Help Search Causes

Applications

Find your way back to Causes: Add Bookmark

Save The Seals

To Stop The Harp Seal Hunt Learn More

9 members • $25 raised

Join Cause

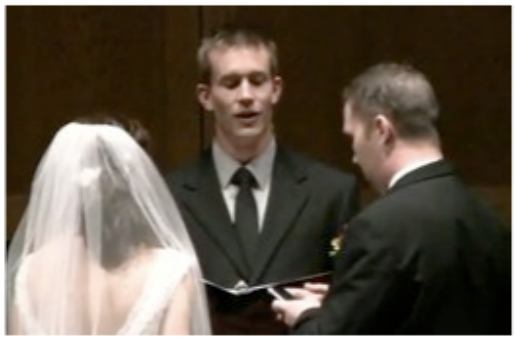
Home About Members Impact

Effective online protest is badly needed

Just Married: Groom Changes Facebook Relationship Status at the Altar [VIDEO]

We've seen plenty of Twittered marriage proposals, but a recent video posted to YouTube takes the cake for the most unconventional Twitter and Facebook update.

During his wedding ceremony, Dana Hanna whipped out his mobile device and not only changed his relationship status to married on Facebook, but also sent out a tweet announcing that the couple had become man and wife.



- Everything else moving online
- Powerful organisations have increasingly little physical presence
- Social movements are increasingly dispersed physically

Critical Art Ensemble, 1996

Effective online protest is badly needed

- Everything else moving online
- Powerful organisations have increasingly little physical presence
- Social movements are increasingly dispersed physically

Critical Art Ensemble, 1996

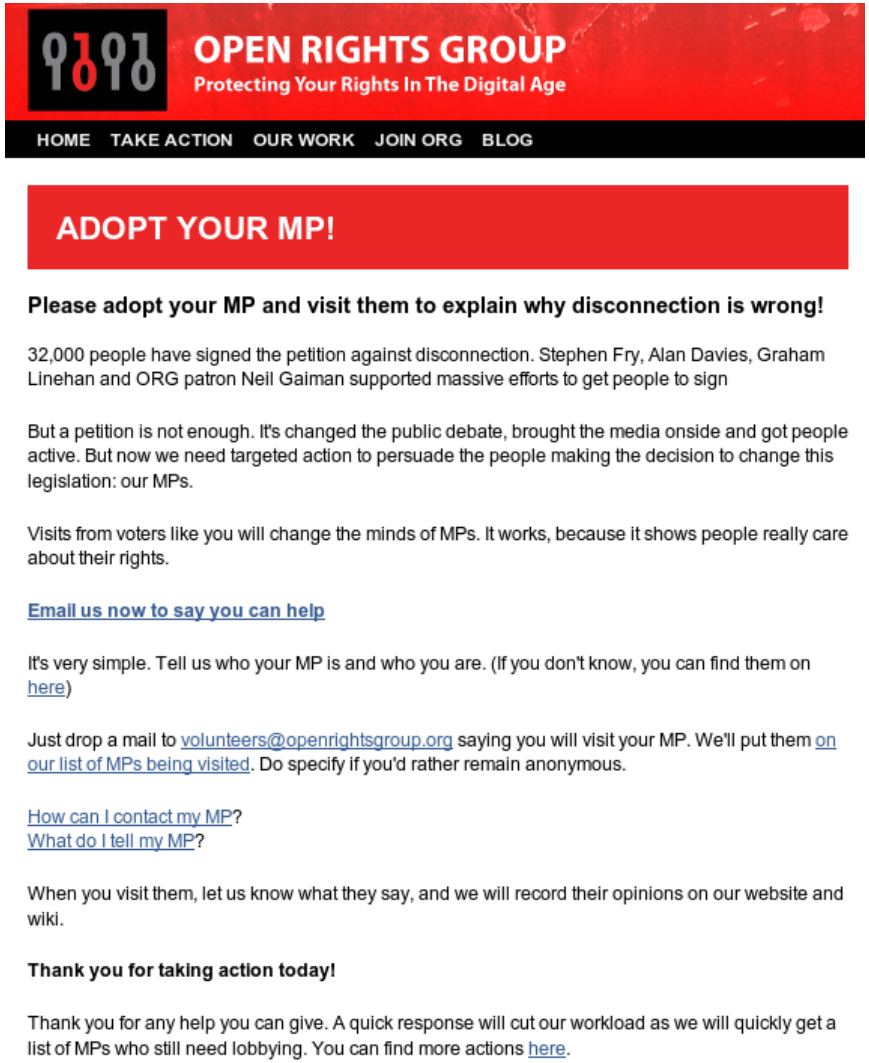
Effective online protest is badly needed

- Everything else moving online
- Powerful organisations have increasingly little physical presence
- Social movements are increasingly dispersed physically

Critical Art Ensemble, 1996

Denning's taxonomy of digital movements

1. **Online Activism**
   - Education & awareness building
   - Fundraising
   - Petitions
   - C & C
2. **Hacktivism**
   - Denial of service
   - Mail bombs
   - Google bombs
   - Website defacement
   - Harassment & "griefing"
3. **Cyber-terrorism**
   - Triggering physical violence



OPEN RIGHTS GROUP
Protecting Your Rights In The Digital Age

HOME TAKE ACTION OUR WORK JOIN ORG BLOG

ADOPT YOUR MP!

Please adopt your MP and visit them to explain why disconnection is wrong!

32,000 people have signed the petition against disconnection. Stephen Fry, Alan Davies, Graham Linehan and ORG patron Neil Gaiman supported massive efforts to get people to sign

But a petition is not enough. It's changed the public debate, brought the media onside and got people active. But now we need targeted action to persuade the people making the decision to change this legislation: our MPs.

Visits from voters like you will change the minds of MPs. It works, because it shows people really care about their rights.

Email us now to say you can help

It's very simple. Tell us who your MP is and who you are. (If you don't know, you can find them on here)

Just drop a mail to volunteers@openrightsgroup.org saying you will visit your MP. We'll put them on our list of MPs being visited. Do specify if you'd rather remain anonymous.

How can I contact my MP?
What do I tell my MP?

When you visit them, let us know what they say, and we will record their opinions on our website and wiki.

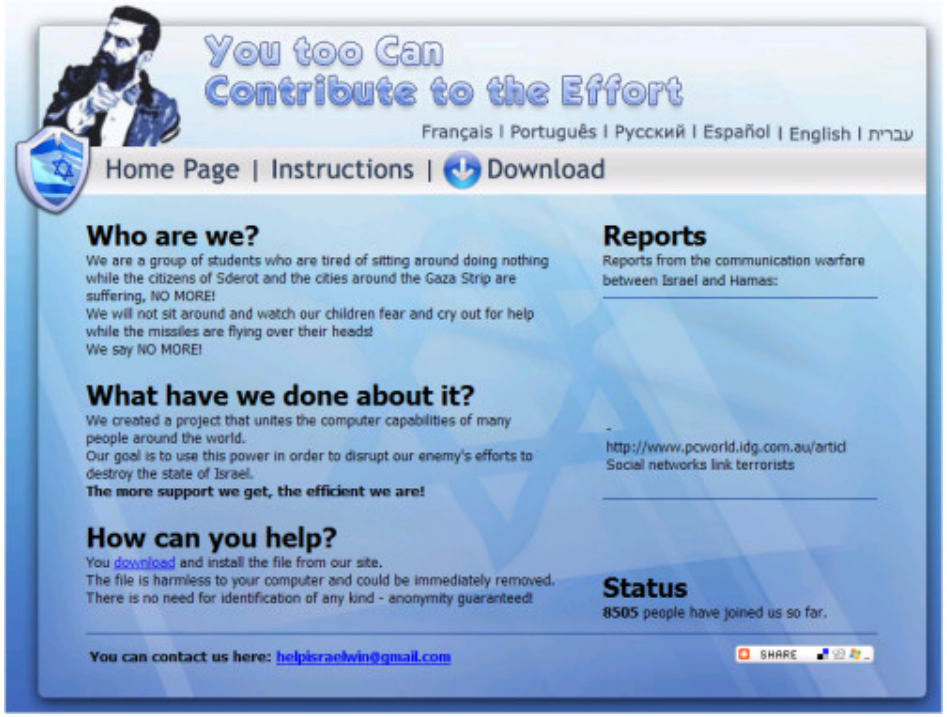
Thank you for taking action today!

Thank you for any help you can give. A quick response will cut our workload as we will quickly get a list of MPs who still need lobbying. You can find more actions here.

Open Rights Group, UK, 2010

Denning's taxonomy of digital movements

1. **Online Activism**
   - Education & awareness building
   - Fundraising
   - Petitions
   - C & C
2. **Hacktivism**
   - Denial of service
   - Mail bombs
   - Google bombs
   - Website defacement
   - Harassment & "griefing"
3. **Cyber-terrorism**
   - Triggering physical violence



Help Israel Win, 2009

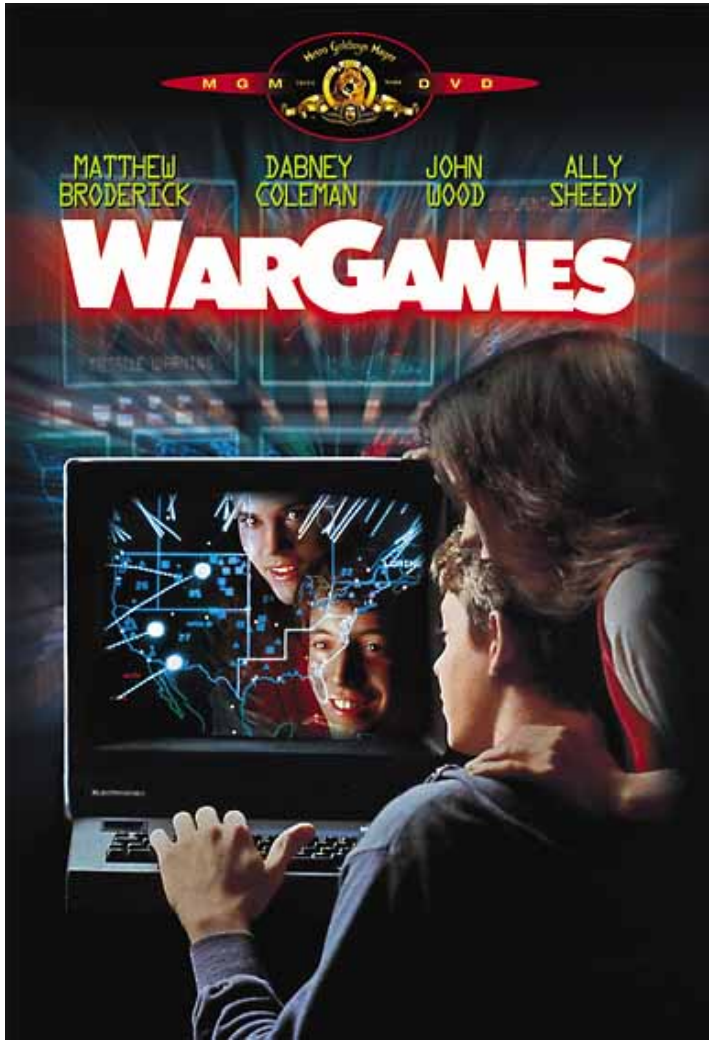
Denning's taxonomy of digital movements

1. **Online Activism**
   - Education & awareness building
   - Fundraising
   - Petitions
   - C & C
2. **Hacktivism**
   - Denial of service
   - Mail bombs
   - Google bombs
   - Website defacement
   - Harassment & "griefing"
3. **Cyber-terrorism**
   - Triggering physical violence

"Iranian Cyber Army", 2009

Denning's taxonomy of digital movements

1. **Online Activism**
   - Education & awareness building
   - Fundraising
   - Petitions
   - C & C
2. **Hacktivism**
   - Denial of service
   - Mail bombs
   - Google bombs
   - Website defacement
   - Harassment & "griefing"
3. **Cyber-terrorism**
   - Triggering physical violence



WarGames (film), 1983

Effective protest usually demonstrates two things

1. **Morality**
   - Non-violence, solidarity, democracy
2. **Commitment**
   - Number of supporters
   - Level of dedication to cause

Effective protest usually demonstrates two things

1. **Morality**
   - Non-violence, solidarity, democracy
2. **Commitment**
   - Number of supporters
   - Level of dedication to cause

Morality

The man who strikes first admits that his ideas have given out.

-Chinese proverb

There is no such thing as defeat in non-violence.

-César Chávez

I have nothing new to teach the world. Truth and non-violence are as old as the hills.

-Mohandas Gandhi

Adherents believe hacktivism is non-violent

WARNING: This is a Protest, it is not a game, it may have personal consequences as in any off-line political manifestation on the street:

1. Your IP address will be harvested by the government during any FloodNet action...(Similar to having your picture taking during a protest action on the street.)
2. Possible damage to your machine may occur because of your participation in the FloodNet action. (Just as in a street action -the police may come and hurt you.)
3. FloodNet clogs bandwidth and may make it difficult for individuals to get information. (This also happens when people take to the streets. Individuals may find themselves unable to get to work because of the action.)

We hope that when you join our Virtual Sit-in's in support of global communities of resistance, you will take the above information to heart.

Electronic Disturbance Theatre, 1999

Commitment

Celebrating the 9/12 rallies; Turnout estimated at 2 million

By Michelle Malkin • September 12, 2009 10:06 AM

Twitpic via **Brooks Bayne**

The New York Times

Politics

Thousands Rally in Capital to Protest Big Government

Amanda Lucidon for The New York Times

A crowd marched toward the Capitol as people from around the country gathered to express their discontent with the government. More Photos >

By JEFF ZELENY
Published: September 12, 2009

9/12 “Tea-Party” march
Washington, DC, USA, 2009

Numbers don’t always indicate commitment

Numbers don’t always indicate commitment

Live 8
London, UK 2005

NY Philharmonic
New York, NY, USA, 2007

Commitment by overcoming opposition

Civil rights marches
Birmingham, AL, USA, 1963

Commitment by overcoming opposition

Anti-WTO protests
Seattle, WA, USA, 1999

Commitment by overcoming opposition

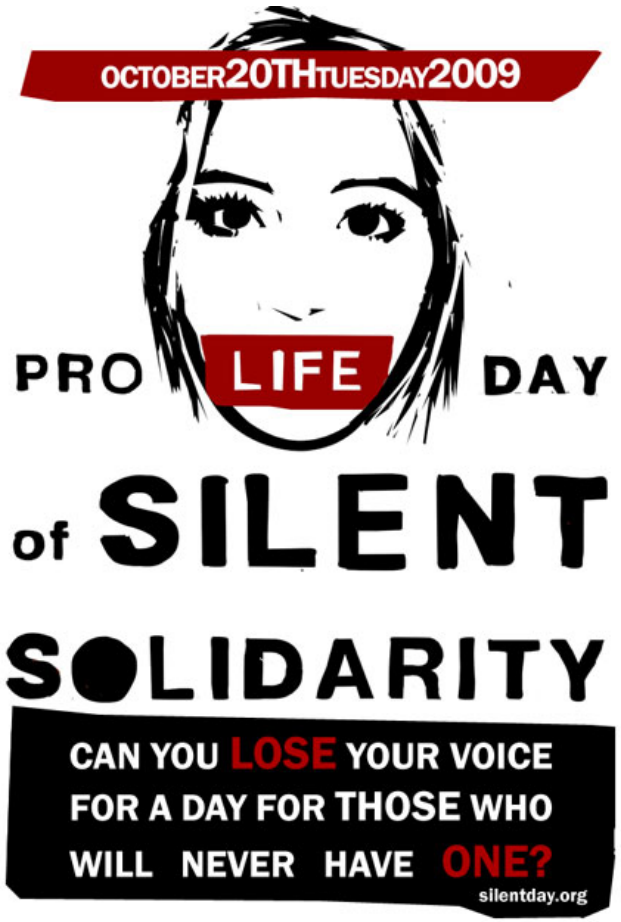
Boston Massacre

Boston, MA, USA, 1770

Commitment by voluntary sacrifice

PETA animal rights protest
Barcelona, Spain, 2007

Commitment by voluntary sacrifice

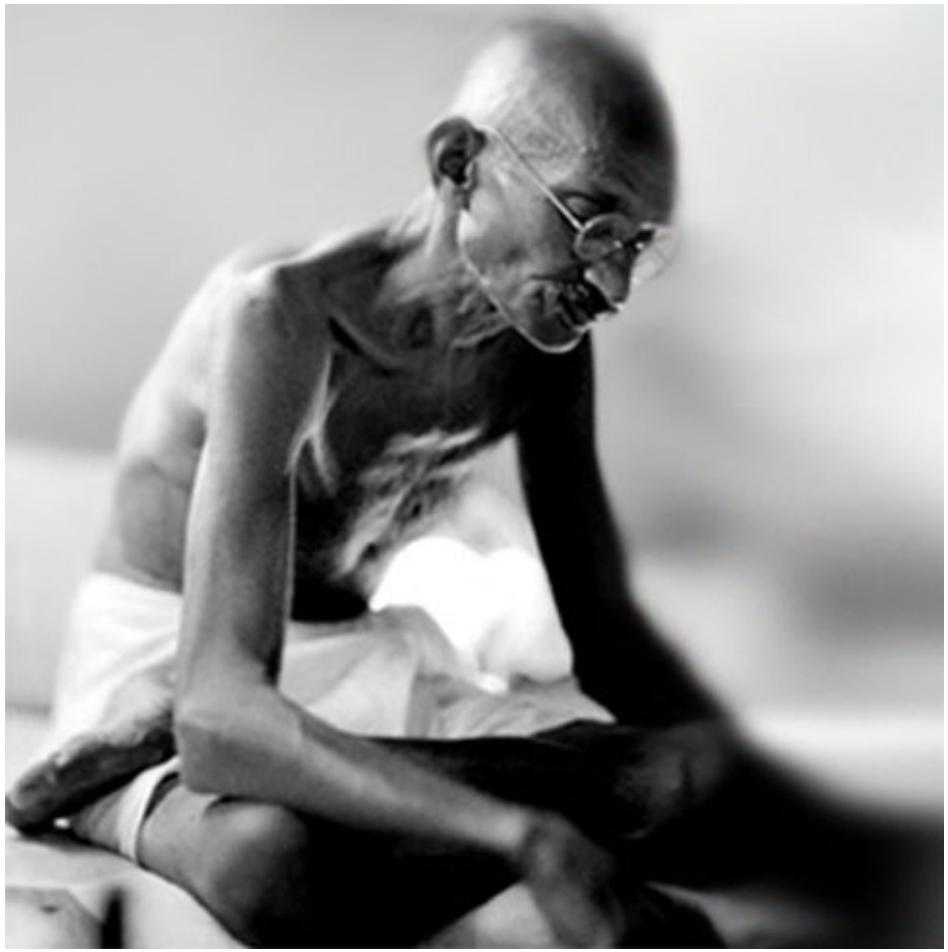


Silent Day pro-life protest
USA, 2009

Commitment by voluntary sacrifice

Anti-government “blood protests”
Bangkok, Thailand, 2010

Commitment by voluntary sacrifice



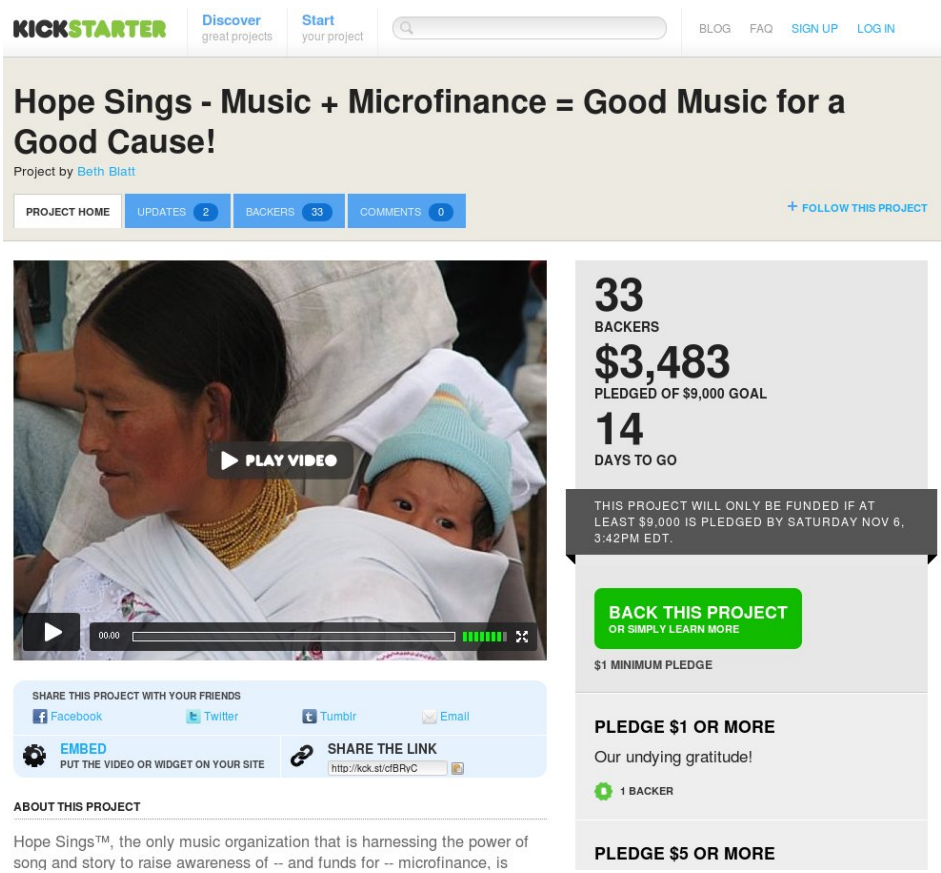
Mohandas Gandhi on hunger strike
Delhi, India, 1948

Commitment by voluntary sacrifice

Self-immolation of Thích Quảng Đức
Saigon, Vietnam, 1963

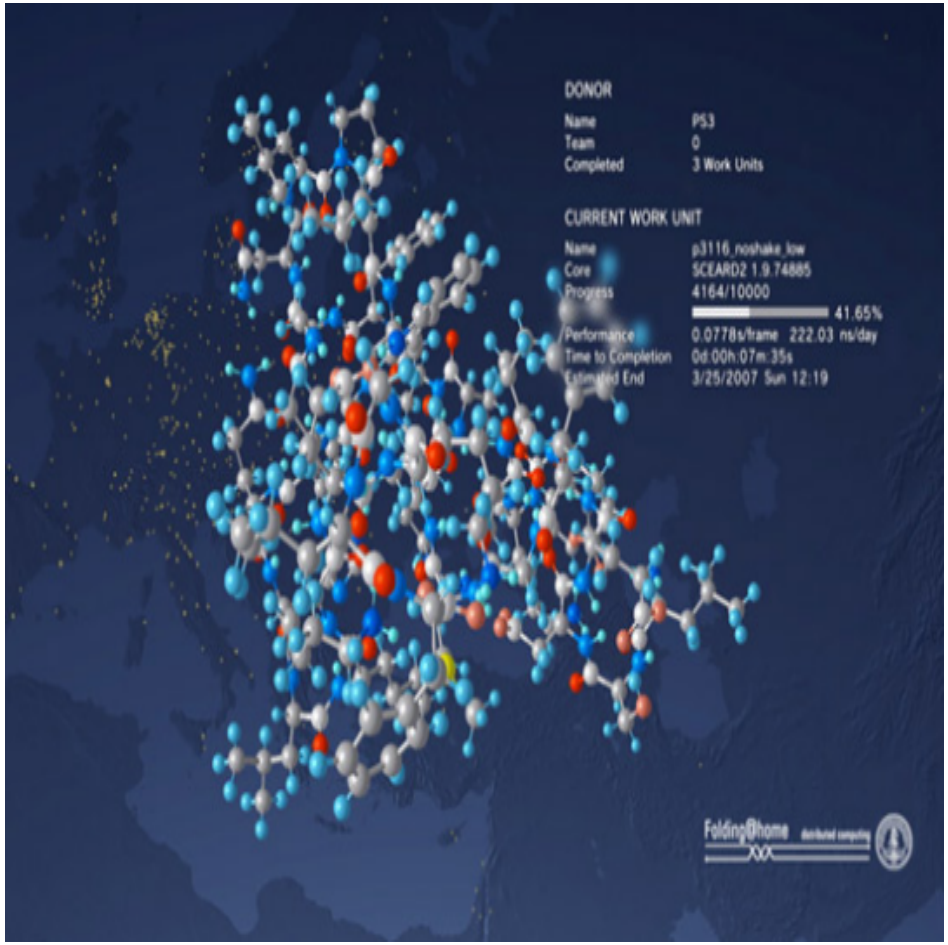
Proving commitment online is hard

1. **Money**
2. CPU cycles
3. Traffic
4. Authority
5. Identity



Proving commitment online is hard

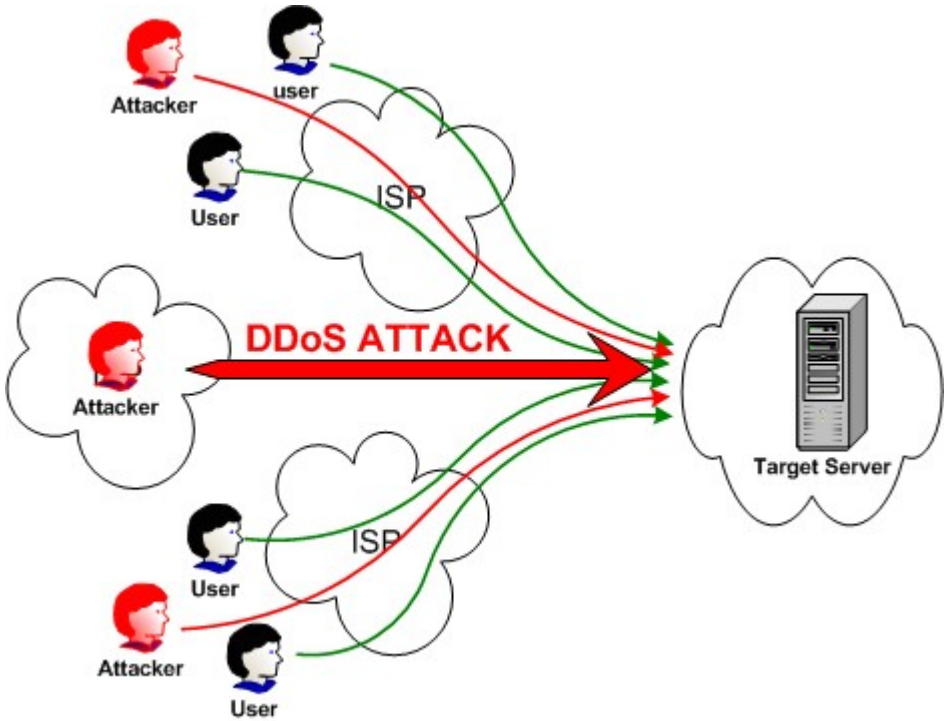
1. **Money**
2. **CPU cycles**
3. Traffic
4. Authority
5. Identity



Folding at Home

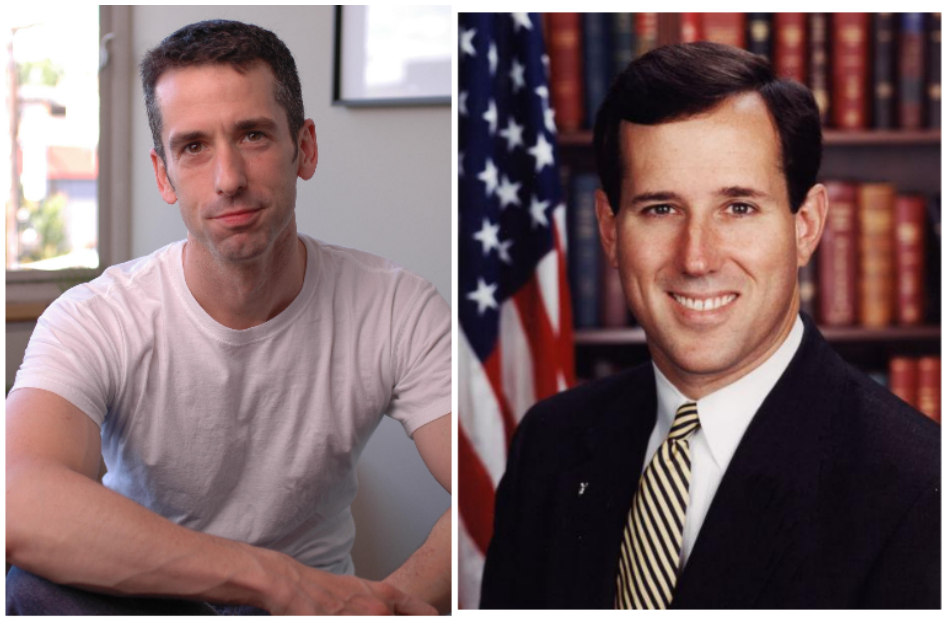
Proving commitment online is hard

1. **Money**
2. **CPU cycles**
3. **Traffic**
4. **Authority**
5. **Identity**



Proving commitment online is hard

1. **Money**
2. **CPU cycles**
3. **Traffic**
4. **Authority**
5. **Identity**



santorum Search

About 730,000 results (0.21 seconds) Advanced search

Santorum (sexual neologism) - Wikipedia, the free encyclopedia

Santorum is a sexual neologism proposed by American humorist and sex-advice columnist Dan Savage in 2003 to "memorialize" then-US Republican senator Rick ...

Background - Contest - Web activism - Political impact

en.wikipedia.org/wiki/**Santorum**_(sexual_neologism) - Cached - Similar

Rick **Santorum** - Wikipedia, the free encyclopedia

Richard John "Rick" **Santorum** (born May 10, 1958) is a former United States ...

en.wikipedia.org/wiki/Rick_**Santorum** - Cached - Similar

Proving commitment online is hard

1. **Money**
2. **CPU cycles**
3. **Traffic**
4. **Authority**
5. **Identity**

People are trying to use their identity

Kimberley Hussein Grant Add as Friend

Wall | Info | Photos | Boxes

Kimberley only shares some of her profile information with everyone. If you know Kimberley, send her a message or add her as a friend.

Basic Information

Networks: Oregon Alum '08
Sex: Female

Send Kimberley a Message
Poke Kimberley

The New York Times

Politics

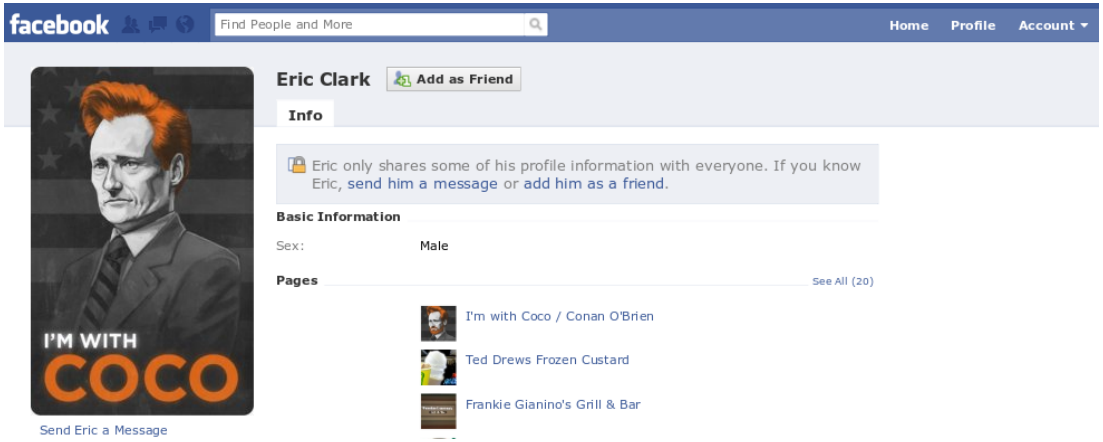
Obama Supporters Take His Name as Their Own

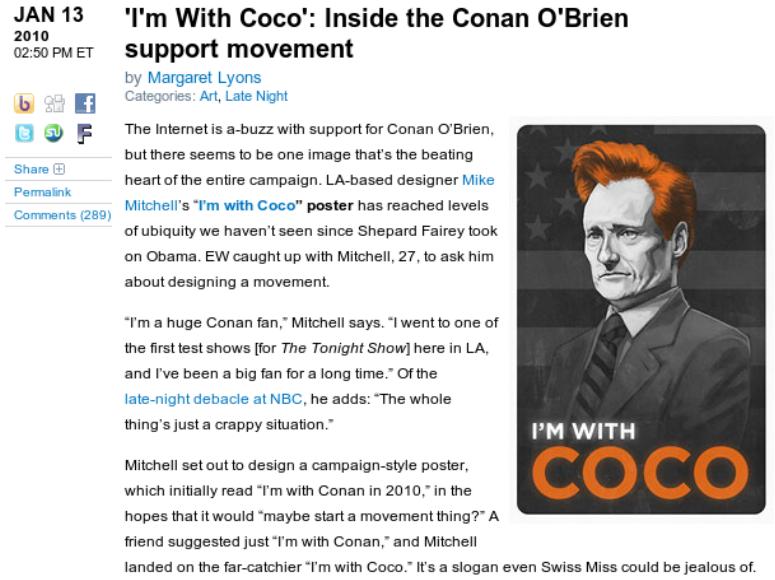
Kirk Irwin for The New York Times

Obama volunteers from Columbus, Ohio, who have adopted the middle name Hussein include J. T. Marcum, left, Aaron Barclay, Alex Enderle, Norm Shoemaker and Chelsey McCune. They use the name on the Internet and in greeting one another.

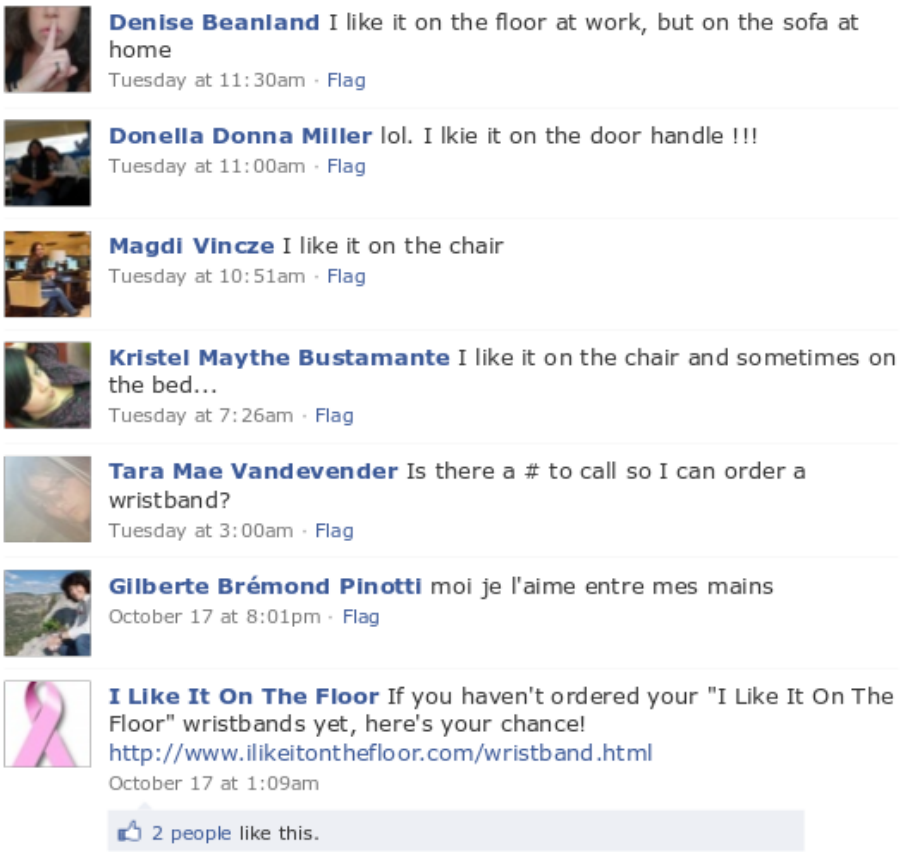
By JODI KANTOR
Published: June 29, 2008

People are trying to use their identity





People are trying to use their identity



Denise Beanland I like it on the floor at work, but on the sofa at home
Tuesday at 11:30am · Flag

Donella Donna Miller lol. I lkie it on the door handle !!!
Tuesday at 11:00am · Flag

Magdi Vincze I like it on the chair
Tuesday at 10:51am · Flag

Kristel Maythe Bustamante I like it on the chair and sometimes on the bed...
Tuesday at 7:26am · Flag

Tara Mae Vandevender Is there a # to call so I can order a wristband?
Tuesday at 3:00am · Flag

Gilberte Brémond Pinotti moi je l'aime entre mes mains
October 17 at 8:01pm · Flag

I Like It On The Floor If you haven't ordered your "I Like It On The Floor" wristbands yet, here's your chance!
http://www.ilikeitonthefloor.com/wristband.html
October 17 at 1:09am

2 people like this.

I changed my status to the color of my bra to support breast cancer <3

Wall | Info | Photos | Discussions

Cryptographers can make things official

- *N* Protesters submit a (valuable) digital identity
  - SNS profile
  - Webmail account
  - Online market reputation
  - Virtual world avatar
- All identites are **locked** during protest
  - Cannot be used/accessed/updated
- *k* of *N* protesters must vote to end the protest
  - Binding solidarity
- Possibility of permanent loss

Cryptographers can make things official

- *N* Protesters submit a (valuable) digital identity
  - SNS profile
  - Webmail account
  - Online market reputation
  - Virtual world avatar
- All identites are **locked** during protest
  - Cannot be used/accessed/updated
- *k* of *N* protesters must vote to end the protest
  - Binding solidarity
- Possibility of permanent loss

Cryptographers can make things official

- *N* Protesters submit a (valuable) digital identity
  - SNS profile
  - Webmail account
  - Online market reputation
  - Virtual world avatar
- All identites are **locked** during protest
  - Cannot be used/accessed/updated
- *k* of *N* protesters must vote to end the protest
  - Binding solidarity
- Possibility of permanent loss

Cryptographers can make things official

- *N* Protesters submit a (valuable) digital identity
  - SNS profile
  - Webmail account
  - Online market reputation
  - Virtual world avatar
- All identites are **locked** during protest
  - Cannot be used/accessed/updated
- *k* of *N* protesters must vote to end the protest
  - Binding solidarity
- Possibility of permanent loss

Cryptographic details

1. Setup
   - P generates a master key pair $(k_*^{\text{pub}}, k_*^{\text{priv}})$
   - P generates N shares $s_1 \ldots s_N$ of k_*^{priv}
   - P generates a symmetric escrow key k_{e}
2. Registration
   - Each protester p_i sends password x_i to P
   - P checks validity of i
   - P sends ZKP(x_i) to $\mathcal{O}$, updates password to random x_i'
   - P sends a share s_i of k_*^{priv} to p_i
3. Protest
   - P signs & publishes:

$$\left\{ \mathrm{E}_{k_{\text{e}}} \left(\mathrm{E}_{k_i^{\text{pub}}}(x_i') \right) \middle| 1 \leq i \leq n \right\}, \quad \mathrm{E}_{k_*^{\text{pub}}}(k_{\text{e}})$$

   - P destroys k_*^{priv}, k_{e}
4. Completion
   - P generates two escrow keys $k_{\text{e}+}^i$ and $k_{\text{e}-}^i$ **per protester**
   - P signs & publishes:

$$\left\{ \mathrm{E}_{k_{\text{e}+}} \left(\mathrm{E}_{k_i^{\text{pub}}}(x_i') \right), \mathrm{E}_{k_{\text{e}-}}(y_i'), \mathrm{E}_{k_*^{\text{pub}}}(k_{\text{e}+}^i), \mathrm{E}_{k_*^{\text{pub}}}(k_{\text{e}-}^i) \middle| 1 \leq i \leq n \right\}$$

Basic protocol enables boycott-style protest

Montgomery bus boycotts
Montgomery, AL, USA, 1955-1956

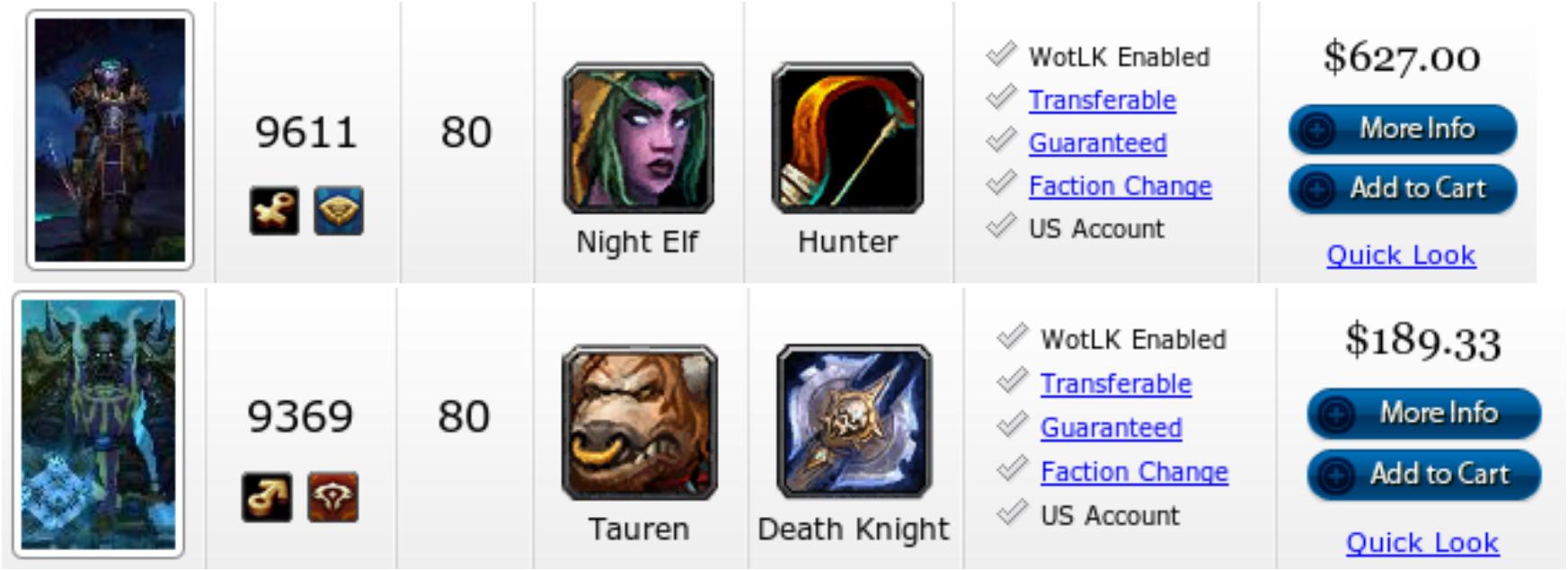
Additional property: binding solidarity

Bio 2004 International Convention protests
San Francisco, CA, USA, 2004

Can also permanently destroy identities

Irish hunger strikes
HM Prison Maze, Belfast, UK, 1981

Many open questions about sacrificing online identities



World of Warcraft characters for sale

Differing value of identities

Many open questions about sacrificing online identities

Friendster

Cost of replacing identities

Many open questions about sacrificing online identities

PAGE ONE | JULY 12, 2007

Whole Foods Is Hot, Wild Oats a Dud -- So Said 'Rahodeb'

Then Again, Yahoo Poster Was a Whole Foods Staffer, The CEO to Be Precise

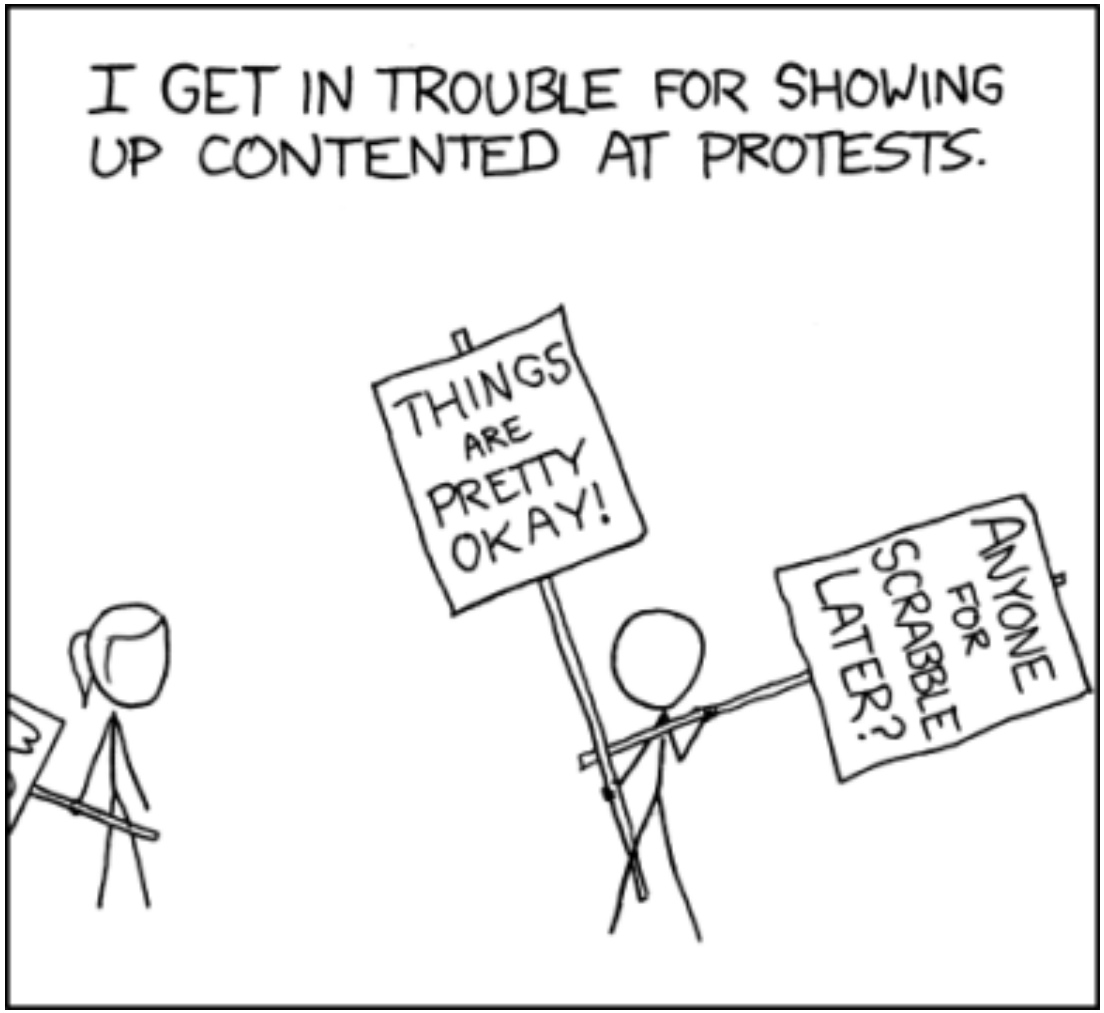
Ability to create multiple identities (sybils)

Many open questions about sacrificing online identities

Kent State anti-war protests
Kent, OH, USA, 1970

Loss of emotional connection

Questions?



xkcd

Protocol details—participants

Password oracle $\mathcal{O}$

- Maintains password table $T : \mathbb{Z} \to \{0,1\}^*$
- Will update $T[i]$ given $(i, \mathrm{ZKP}(T[i]), T[i]')$
- Must be **indifferent** to goals of protest

Protocol details—participants

Protesters $p_1 \ldots p_N$

- Each has a password x_i registered with $\mathcal{O}$
- Also has a key pair $(k_*^{\text{pub}}, k_*^{\text{priv}})$

Protocol details—participants

Protest initiator P

- Has a known public key k_P^{pub}
- Must be **trusted** by all protesters

Protocol details—cryptography

1. Setup
   - P generates a master key pair $(k_*^{\text{pub}}, k_*^{\text{priv}})$
   - P generates N shares $s_1 \ldots s_N$ of k_*^{priv}
   - P generates a symmetric escrow key k_e
2. Registration
   - Each protester p_i sends password x_i to P
   - P checks validity of i
   - P sends ZKP(x_i) to O, updates password to random x_i'
   - P sends a share s_i of k_*^{priv} to p_i
3. Protest
   - P signs & publishes:

$$\left\{ E_{k_e}\left(E_{k_i^{\text{pub}}}(x_i') \right) \middle| 1 \le i \le n \right\}, \quad E_{k_*^{\text{pub}}}(k_e)$$

   - P destroys k_*^{priv}, k_e
4. Completion
   - Protest ends when t protesters agree to decrypt k_e

Protocol details—cryptography

1. Setup
   - P generates a master key pair $(k_*^{\text{pub}}, k_*^{\text{priv}})$
   - P generates N shares $s_1 \ldots s_N$ of k_*^{priv}
   - P generates a symmetric escrow key k_e
2. Registration
   - Each protester p_i sends password x_i to P
   - P checks validity of i
   - P sends ZKP(x_i) to $\mathcal{O}$, updates password to random x_i'
   - P sends a share s_i of k_*^{priv} to p_i
3. Protest
   - P signs & publishes:

$$\left\{ E_{k_e}\left(E_{k_i^{\text{pub}}}(x_i') \right) \middle| 1 \le i \le n \right\}, \quad E_{k_*^{\text{pub}}}(k_e)$$

   - P destroys k_*^{priv}, k_e
4. Completion
   - Protest ends when t protesters agree to decrypt k_e

Protocol details—cryptography

1. Setup
   - P generates a master key pair $(k_*^{\text{pub}}, k_*^{\text{priv}})$
   - P generates N shares $s_1 \ldots s_N$ of k_*^{priv}
   - P generates a symmetric escrow key k_e
2. Registration
   - Each protester p_i sends password x_i to P
   - P checks validity of i
   - P sends ZKP(x_i) to $\mathcal{O}$, updates password to random x_i'
   - P sends a share s_i of k_*^{priv} to p_i
3. Protest
   - P signs & publishes:

$$\left\{ \mathrm{E}_{k_e}\left(\mathrm{E}_{k_i^{\text{pub}}}(x_i')\right) \middle| 1 \leq i \leq n \right\}, \quad \mathrm{E}_{k_*^{\text{pub}}}(k_e)$$

   - P destroys k_*^{priv}, k_e
4. Completion
   - Protest ends when t protesters agree to decrypt k_e

Protocol details—cryptography

1. Setup
   - P generates a master key pair $(k_*^{\text{pub}}, k_*^{\text{priv}})$
   - P generates N shares $s_1 \ldots s_N$ of k_*^{priv}
   - P generates a symmetric escrow key k_e
2. Registration
   - Each protester p_i sends password x_i to P
   - P checks validity of i
   - P sends ZKP(x_i) to $\mathcal{O}$, updates password to random x_i'
   - P sends a share s_i of k_*^{priv} to p_i
3. Protest
   - P signs & publishes:

$$\left\{ \mathrm{E}_{k_e}\left(\mathrm{E}_{k_i^{\text{pub}}}(x_i')\right) \middle| 1 \leq i \leq n \right\}, \quad \mathrm{E}_{k_*^{\text{pub}}}(k_e)$$

   - P destroys k_*^{priv}, k_e
4. Completion
   - Protest ends when t protesters agree to decrypt k_e

Protocol details—group suicide

Irish hunger strike

HM Prison Maze, Belfast, UK, 1981

- P generates two escrow keys k_{e+} and k_{e-}
- P signs & publishes:

$$\left\{ \mathrm{E}_{k_{e+}} \left(\mathrm{E}_{k_i^{\mathrm{pub}}}(x_i') \right), \mathrm{E}_{k_{e-}}(y_i') \middle| 1 \leq i \leq n \right\}, \quad \mathrm{E}_{k_*^{\mathrm{pub}}}(k_{e+}), \mathrm{E}_{k_*^{\mathrm{pub}}}(k_{e-})$$

- y_i' is an **account destruction** key
  - Not protected by p_i's private key
  - May be explicitly provided by $\mathcal{O}$, or be x_i' if we trust griefers

Protocol details—individual destruction

Boston Massacre

Boston, MA, USA, 1770

- P generates two escrow keys $k^i_{\mathrm{e}+}$ and $k^i_{\mathrm{e}-}$ **per protester**
- P signs & publishes:

$$\left\{ \mathrm{E}_{k_{\mathrm{e}+}} \left(\mathrm{E}_{k_i^{\mathrm{pub}}}(x'_i) \right), \mathrm{E}_{k_{\mathrm{e}-}}(y'_i), \mathrm{E}_{k_*^{\mathrm{pub}}}(k^i_{\mathrm{e}+}), \mathrm{E}_{k_*^{\mathrm{pub}}}(k^i_{\mathrm{e}-}) \middle| 1 \leq i \leq n \right\}$$

- Individual accounts can be unlocked or destroyed
  - May choose accounts at random to destroy at regular intervals

Limitations

Indifference of $\mathcal{O}$

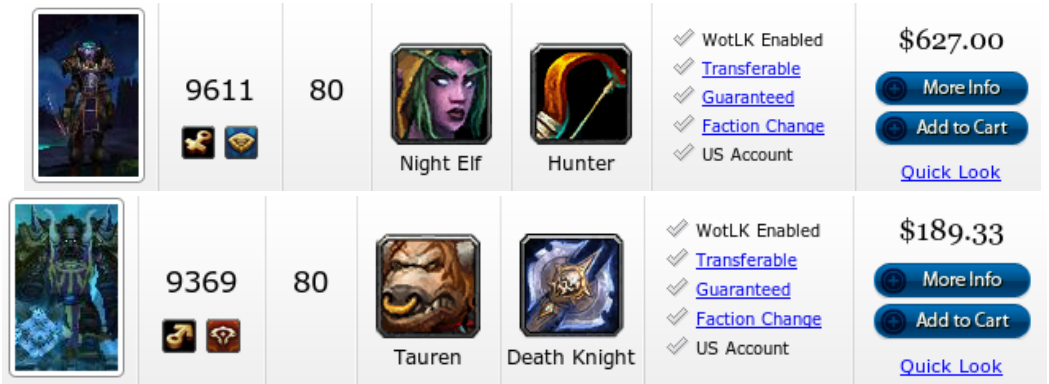
- Can't protest against platform operator itself
- $\mathcal{O}$ can block password updates, reinstate deleted accounts

Limitations

Minority of platform users involved

- $\mathcal{O}$ will block a protest which costs it too much
- Less commitment shown if all users leave at once

Limitations



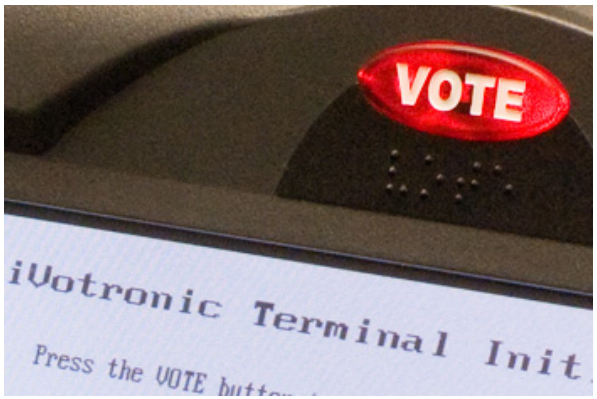
Value of online identities

- Real-world protest holds all lives to have equal value
- Online identities only valuable if built up over time

Limitations

Central trust

- Hard to avoid due to circular dependencies during inititiation
  - Distributed protocol possible?
- *P* can go offline after initialisation
  - Replace *P* with an HSM?



Voting Issues

- Threshold Decryption $\neq$ voting
  - Need a robust, homomorphic scheme, at minimum
- Infiltration/sybil attacks
  - Acquire many shares (votes) by submitting dummy profiles
- Splinter coalition
  - Conspiracy can secede, refuse to unlock some profiles