New directions in online protest

Joseph Bonneau

jcb82@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

18th International Workshop on Security Protocols

Cambridge, UK

March 24, 2010

What's wrong with the world today?

Developmental Inequality

What’s wrong with the world today?

Climate Change

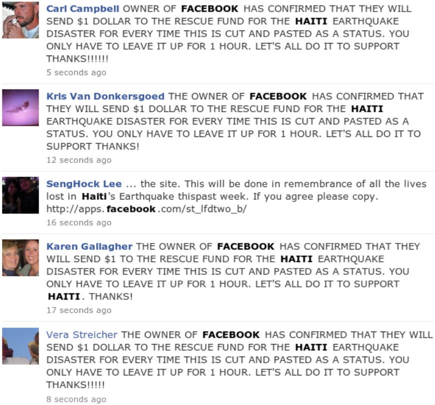
What's wrong with the world today?

Seal Hunting

What’s wrong with the world today?

Conan O’Brien fired by NBC

What's my generation doing about it?



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

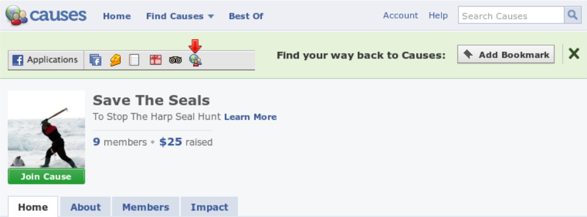
Karen Gallagher THE OWNER OF **FACEBOOK** HAS CONFIRMED THAT THEY WILL SEND $1 TO THE RESCUE FUND FOR THE **HAITI** EARTHQUAKE DISASTER FOR EVERY TIME THIS IS CUT AND PASTED AS A STATUS. YOU ONLY HAVE TO LEAVE IT UP FOR 1 HOUR. LET'S ALL DO IT TO SUPPORT **HAITI**. THANKS!

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

What’s my generation doing about it?

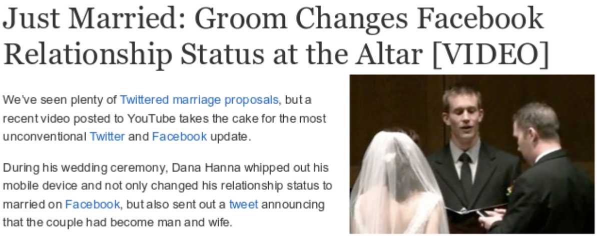


Save The Seals

To Stop The Harp Seal Hunt Learn More

9 members • $25 raised

Reasons to protest online



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

Reasons to protest online

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

Critical Art Ensemble, 1996

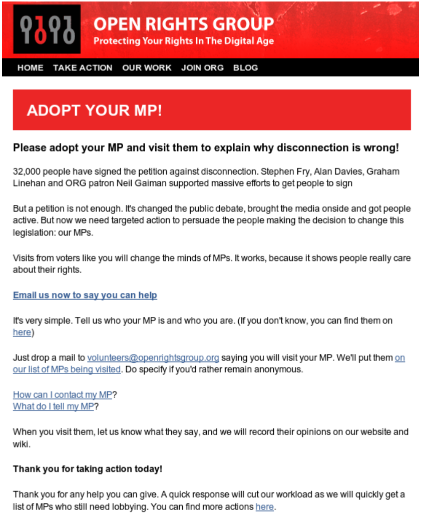
Reasons to protest online

- 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 protest

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



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.

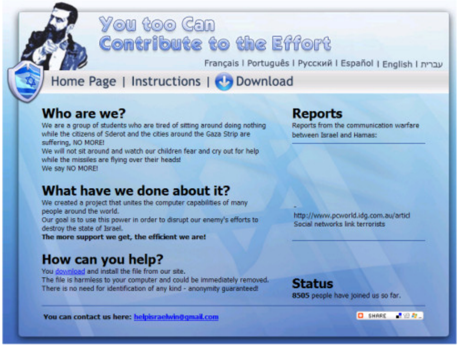
Thank you for taking action today!

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 protest

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


You too Can
Contribute to the Effort
Français I Português I Русский I Español I English I עברית
Home Page | Instructions | Download

Who are we?
We are a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering, NO MORE!
We will not sit around and watch our children fear and cry out for help while the missiles are flying over their heads!
We say NO MORE!

What have we done about it?
We created a project that unites the computer capabilities of many people around the world.
Our goal is to use this power in order to disrupt our enemy's efforts to destroy the state of Israel.
The more support we get, the efficient we are!

How can you help?
You download and install the file from our site.
The file is harmless to your computer and could be immediately removed.
There is no need for identification of any kind - anonymity guaranteed!

Reports
Reports from the communication warfare between Israel and Hamas:

-
http://www.pcworld.idg.com.au/articl
Social networks link terrorists

Status
8505 people have joined us so far.

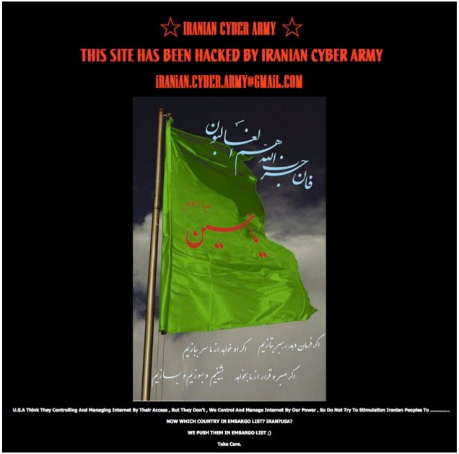
You can contact us here: helpisraelwin@gmail.com

SHARE

Help Israel Win, 2009

Denning's taxonomy of digital protest

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 ☆

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

iRANiAN.CYBER.ARMY@GMAiL.COM

U.S.A Think They Controlling And Managing Internet By Their Access , But They Don't , We Control And Manage Internet By Our Power , So Do Not Try To Stimulation Iranian Peoples To ....

NOW WHICH COUNTRY IN EMBARGO LIST? IRAN?USA?

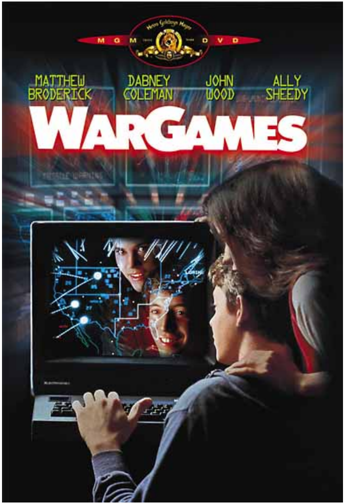
WE PUSH THEM IN EMBARGO LIST ;)

Take Care.

"Iranian Cyber Army", 2009

Denning's taxonomy of digital protest

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

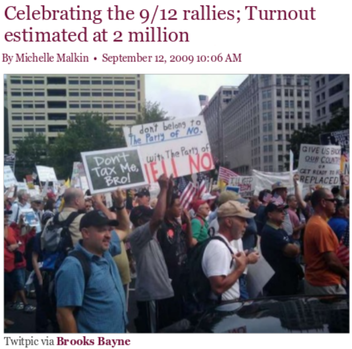
WARNING: This is a Protest, it is not a game, it may have personal consequences as in any off-line political manifestation on the street:

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

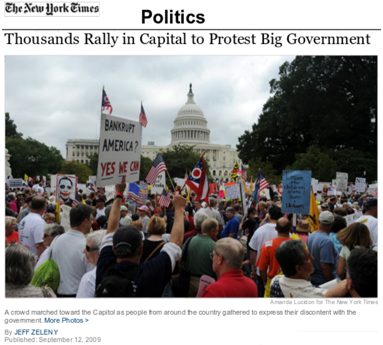


Celebrating the 9/12 rallies; Turnout estimated at 2 million

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

I don't belong to The Party of NO. With The Party of HELL NO
Don't Tax Me, Bro!
GIVE US BACK OUR COUNTRY or GET READY TO BE REPLACED

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

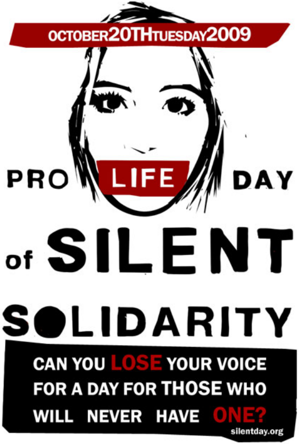
Photo © John Filo

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

Commitment by voluntary sacrifice

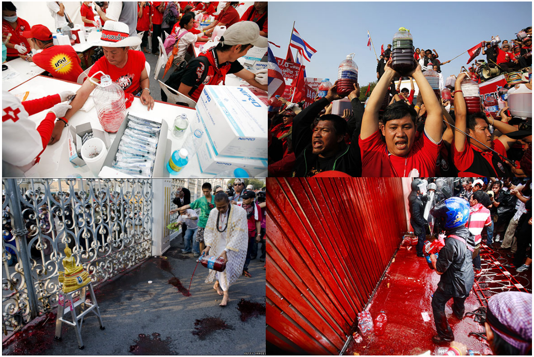
PETA animal rights protest
Barcelona, Spain, 2007

Commitment by voluntary sacrifice



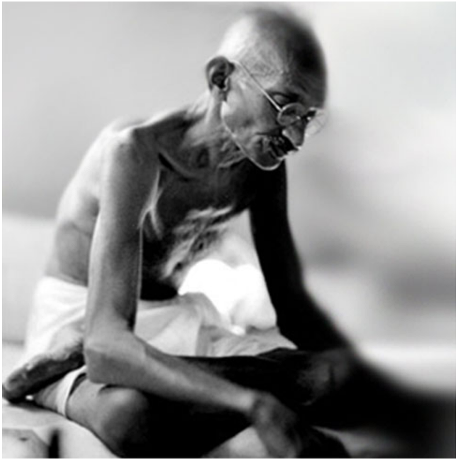
Silent Day pro-life protest
USA, 2009

Commitment by voluntary sacrifice



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

Commitment by voluntary sacrifice



Mohandas Gandhi on hunger strike
Delhi, India, 1948

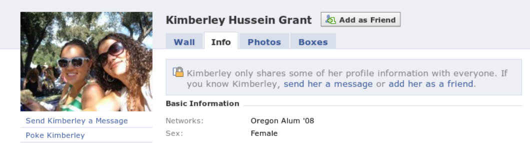
Commitment by voluntary sacrifice

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

Better digital protest

- Want real commitment
- What can one sacrifice online?

Fledgling efforts at commitment in online protest

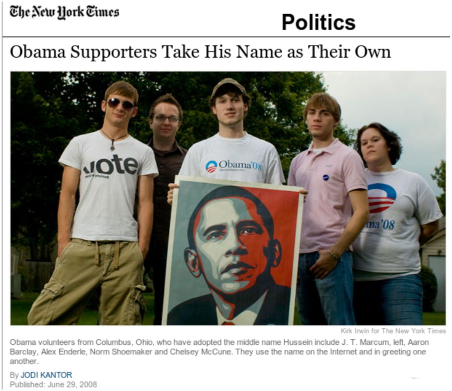


Kimberley Hussein Grant

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



The New York Times

Politics

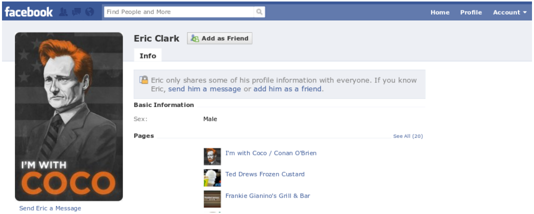
Obama Supporters Take His Name as Their Own

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

Fledgling efforts at commitment in online protest



Eric Clark Add as Friend

Info

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

Basic Information

Sex: Male

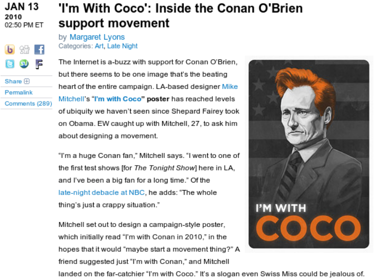
Pages See All (20)

I'm with Coco / Conan O'Brien

Ted Drews Frozen Custard

Frankie Gianino's Grill & Bar

Send Eric a Message



JAN 13
2010
02:50 PM ET

'I'm With Coco': Inside the Conan O'Brien support movement

by Margaret Lyons
Categories: Art, Late Night

The Internet is a-buzz with support for Conan O'Brien, but there seems to be one image that's the beating heart of the entire campaign. LA-based designer Mike Mitchell's "**I'm with Coco**" **poster** has reached levels of ubiquity we haven't seen since Shepard Fairey took on Obama. EW caught up with Mitchell, 27, to ask him about designing a movement.

"I'm a huge Conan fan," Mitchell says. "I went to one of the first test shows [for *The Tonight Show*] here in LA, and I've been a big fan for a long time." Of the late-night debacle at NBC, he adds: "The whole thing's just a crappy situation."

Mitchell set out to design a campaign-style poster, which initially read "I'm with Conan in 2010," in the hopes that it would "maybe start a movement thing?" A friend suggested just "I'm with Conan," and Mitchell landed on the far-catchier "I'm with Coco." It's a slogan even Swiss Miss could be jealous of.

A proposal for committed online protest

- *N* protesters submit a (valuable) digital identity
  - SNS profile
  - Webmail account
  - Online market reputation
  - Virtual world avatar
- All identites are **locked** during protest
- *k* of *N* must vote to end the protest
  - Binding solidarity
- Possibility of permanent loss

A proposal for committed online protest

- *N* protesters submit a (valuable) digital identity
  - SNS profile
  - Webmail account
  - Online market reputation
  - Virtual world avatar
- All identites are **locked** during protest
- *k* of *N* must vote to end the protest
  - Binding solidarity
- Possibility of permanent loss

A proposal for committed online protest

- *N* protesters submit a (valuable) digital identity
  - SNS profile
  - Webmail account
  - Online market reputation
  - Virtual world avatar
- All identites are **locked** during protest
- *k* of *N* must vote to end the protest
  - Binding solidarity
- Possibility of permanent loss

A proposal for committed online protest

- *N* protesters submit a (valuable) digital identity
  - SNS profile
  - Webmail account
  - Online market reputation
  - Virtual world avatar
- All identites are **locked** during protest
- *k* of *N* must vote to end the protest
  - Binding solidarity
- Possibility of permanent loss

Protocol participants

Password oracle $\mathcal{O}$

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

Protocol participants

facebook

Name:
Fareeza Suhaimi

Email:
affareeza@hotmail.com

Status:
Teringat ada orang kata, kite-kite ni kalau plan...

Jonathan T.

Michael M.
Artist from Portland, OR

My blog: Understanding Color

About Michael
I grew up in Boston, but I've been working in Portland for the past few years as an independent artist.

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 participants

Protest initiator *P*

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

Basic protest protocol

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:

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

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

Basic protest protocol

1. Setup
   - P generates a master key pair $(k_*^{\text{pub}}, k_*^{\text{priv}})$
   - P generates N shares $s_1 \dots s_N$ 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:

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

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

Basic protest protocol

1. Setup
   - P generates a master key pair $(k_*^{\mathrm{pub}}, k_*^{\mathrm{priv}})$
   - 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:

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

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

Basic protest protocol

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
   - Protest ends when t protesters agree to decrypt k_e

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

Modified protocol enables group suicide

Irish hunger strike

HM Prison Maze, Belfast, UK, 1981

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

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

- 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

Further modifications allow individual destruction

Boston Massacre

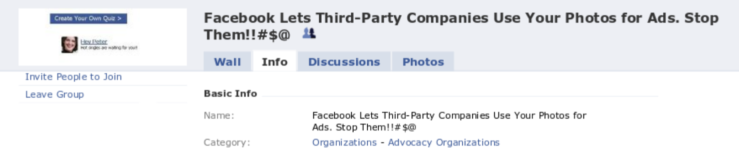
Boston, MA, USA, 1770

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

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

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

Limitations



Facebook Lets Third-Party Companies Use Your Photos for Ads. Stop Them!!#$@

Basic Info

Name: Facebook Lets Third-Party Companies Use Your Photos for Ads. Stop Them!!#$@

Category: Organizations - Advocacy Organizations

Indifference of $\mathcal{O}$

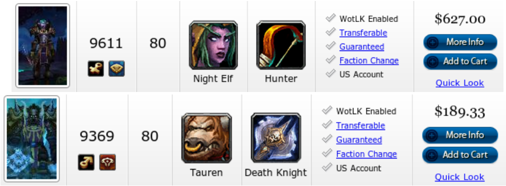
- Can’t protest against platform operator itself
- $\mathcal{O}$ can block password updates, reinstate deleted accounts

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



	9611	80	Night Elf	Hunter	✓ WotLK Enabled ✓ Transferable ✓ Guaranteed ✓ Faction Change ✓ US Account	$627.00 More Info Add to Cart Quick Look
	9369	80	Tauren	Death Knight	✓ WotLK Enabled ✓ Transferable ✓ Guaranteed ✓ Faction Change ✓ US Account	$189.33 More Info Add to Cart Quick Look

Value of online identities

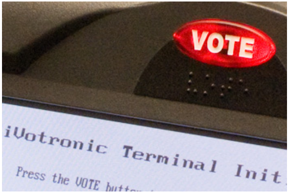
- Real-world protest holds all lives to have equal value
- Online identities only valuable if built up over time

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?

Limitations



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

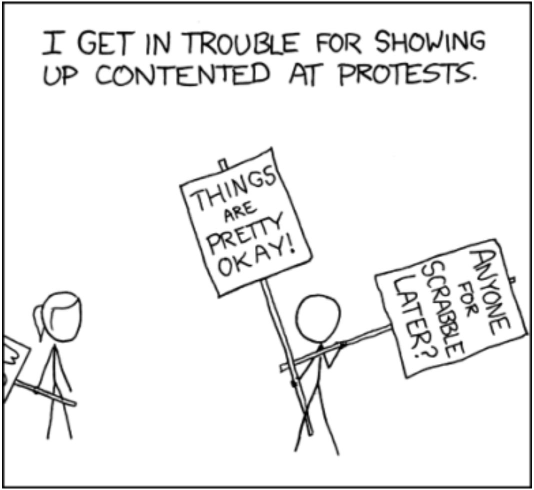
Assessment

1. **Morality**
   - Pretty good
   - Questions about transparency, role of organiser
2. **Commitment**
   - Depends on your point of view...

Assessment

1. **Morality**
   - Pretty good
   - Questions about transparency, role of organiser
2. **Commitment**
   - Depends on your point of view...

Questions?


I GET IN TROUBLE FOR SHOWING UP CONTENTED AT PROTESTS.
THINGS ARE PRETTY OKAY!
ANYONE FOR SCRABBLE LATER?

jcb82@cl.cam.ac.uk