“Kill Switch” or Bait and Switch?

AALS Section on Computers and Internet Law

January 6, 2012

A. Michael Froomkin

University of Miami School of Law

Sympathy for the Devil?

- Opponents of the 'Kill Switch' have, with that name, managed to brand the plan as a terrible idea
- Intellectual challenge is to give the plan a sympathetic reading – *what are they thinking? Is there a point to this?*
- Very hard to achieve – despite best efforts plan seems muddled, wrong-headed, or just possibly worse.

Threat models

- Worms (accidental or intentional)
  - Morris, Stuxnet
- DDoS Attacks (botnets)
- Critical infrastructure sabotage
  - Target-rich environment
    - Internal computer systems
    - Embedded hardware (aka Trojan devices)
      - "Embedded processors and controllers in critical industries" Included in definition of "cyberspace"

Potential sources of threats

- Foreign states
- Foreign terrorists
- Domestic terrorists
- Foreign or domestic blackmailers
- American Spring?

What is in the bill

- Creates two new offices – one in White House to coordinate policy and one in Homeland Security to issue regulations
- Requires (and eliminates judicial review of)
  - Identification of ‘critical infrastructure’
  - Creation of required standards for operation of covered critical infrastruture
  - Drafting of contingency plans to respond to ‘cyber emergency’ (mandatory and exculpatory)

The so-called ‘kill switch’

- President can issue "declaration of cyber emergency" if he certifies
  actual or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure
- Share declaration with Congress, but not public?

Constitutional law aspects

- Bill seeks to make decision unreviewable
- Underlying standards are drafted through combination of rulemaking and secrecy
- 'Nationalization' of internet infrastructure differs from *Steel Seizure* as this is conforming to legislative delegation – presidency at its strongest
  - War power + Congress?
- Even so, can all judicial review be eliminated?

What does that mean?

- What is “exploiting a cyber risk" and what is "critical infrastructure“?
  - “Cyber risk” is anything that
    - “could pose a significant risk of disruption to the operation of information infrastructure essential to the reliable operation of covered critical infrastructure”
  - Which is pretty broad

“Critical infrastructure”

- Those systems whose disruption or destruction would cause a mass casualty event which includes an extraordinary number of fatalities; severe economic consequences; mass evacuations with a prolonged absence; or severe degradation of national security capabilities, including intelligence and defense functions.

Note the breadth

- This list of triggers is very very broad because it is an "or" not an "and" list
  - “Severe economic consequences” – lots of things have those
  - “Severe degradation of national security / intelligence”
    - What they said about encryption (and breaking encryption)
- Also critical infrastructure can include providers of information technology & everyone else involved in internet

Would publishing ever qualify?

- Bill says that means used to respond to cyber emergency must be "least disruptive means possible“
  - NB *means to respond* isn’t issue so much as *what is being responded to*
- Only partial protection for 1st Amendment:
  - Bill prohibits identifying systems or assets as covered critical infrastructure "based solely on activities protected by the" 1st Amendment”
  - Partly is apparently OK?

Hypos

- Which of these are “solely” a First Amendment activity
  - Publishing the Pentagon Papers
  - Publishing the instructions to build an atomic bomb strong (The Nation case)
  - Publishing the algorithm for strong crypto (PGP case)
  - Publishing virus-making info

What plugs could they pull?

- Legislation doesn't say – delegates to Homeland Security
- Consequences of plug-pulling poorly understood
  - My story
    - Phones
    - Finance
    - Skype
    - Email
    - Music

‘Kill Switch’ – possible locations

- Backbone / transport
- Major access providers
- Key web-based services
- End-user hardware
- End-user applications

Backbone / transport layer

- There is an Internet ‘super-highway’
  - Small number of major providers
  - Can be routed around to some extent, but congestion problems would likely be severe
- Sponsors of bill disclaim intent to regulate the backbone (which is somewhat curious)

Major access providers

- Three types (overlapping)
  - ISPs
  - Cell phone service providers
    - Including RIM network
  - Landline service providers
- Substantial concentration (especially cell)
- Very hard to route around – likely a major chokepoint/target for regulation.

Key web-based services

- Varied types
  - Search
  - Social media
  - ‘Cloud’ services
- Easy to target
- Not clear if these targets meet explicit threat models
  - But see UK threats to close RIM/Twitter networks

End-user hardware

- Return of ‘trusted computing’?
- Large installed PC base makes this unlikely to be effective
- Might work for some embedded systems, depending on the technology

End-user applications

- Operating systems?
- Might work if there were an industry that relied heavily on one operating system
- Otherwise, variety of systems makes this of at best partial utility
  - Windows works if your target is the home user

The mystery

- What do they think they are doing?
  - Particularly given existing authority under Communications of Act of 1934 §706
    - Enacted shortly after Pearl Harbor
    - gives the President the power to shut down "any facility or station for wire communication" or take federal control of such facilities in the event of a "state of war" and for up to six months after the expiration of such a state.
  - Committee report says new authority is more ‘fine-tuned’

Why aren't incentives aligned?

- Likely/actual victim of an attack would be highly motivated to cooperate, why require it?
  - Might seek/enjoy some immunities vs. customers for a shutdown
- Potential targets would welcome government advice/standards
  - Might be reluctance to disclose details of operations?

A scenario

- Victim has embedded hardware with Trojan waiting for ‘ping of death’ from foreign source
- Activation instructions pass over 3rd party networks
  - Owner of network not willing to take it all down to prevent harm to Victim’s infrastructure
  - Wants government to step in

Government action

- ID when threat is real
- Force 3rd party to shut down
  - Issue: is minimization of harms possible without deep packet inspection?
- Immunize 3rd party from suit
  - its customers bear losses?
  - Remember how dependent I am on the internet

(Almost) all ‘kill switch’ roads lead to deep packet inspection

- If the plan is to discriminate between ‘dangerous’ and ‘harmless’ content, DPI is the technique of choice
- Is the objective here to require that all intermediary networks be DPI-ready?
  - Or even if not the objective, isn’t this the likely outcome?
- Bill says it doesn’t increase wiretap authority – but DPI/wiretap line is fuzzy

One last problem to worry about

- US sets tech standards that are widely copied
- If we mandate a ‘kill switch’ capacity for key infrastructure that the government can force and/or that all providers and intermediaries be DPI-ready, this will be a gift to authoritarians everywhere as it greatly reduces the cost of Internet control