An Analysis of the Legality of Government-Mandated Computer Inoculations

M. Rice, J. Butts, R. Miller* and S. Shenoi

University of Tulsa
Tulsa, Oklahoma

*National Defense University
Fort McNair
Simple Computer Inoculation (Scenario #1)

- State government mandates computer inoculations
- Vaccination centers are established to inoculate computing resources
- Computer Protection Board
- Cost covered by government (swine flu vaccine) or via subscription fee

Seeks to establish herd immunity in cyberspace through a mass vaccination strategy
Simple Computer Inoculation (Analysis)

• **Governmental Powers**
  - State government: Police Powers
  - Federal government: Commerce Clause (Article I, section 8) and the responsibility to provide for the national defense

• **Position of state government:**
  - Computing resources that connect to the Internet should have “up-to-date” inoculations—similar to states’ position requiring vaccination for school attendance under the police powers doctrine

• **Arguments against mandated inoculations**
• Jacobson v. Massachusetts
  – U.S. Supreme Court, 1905
  – Enabled state legislatures to fight outbreaks by mandating inoculations, but placed some restrictions
  – Shaped public policy – more than 2,500 cases in various courts have referred to this case

• Supreme Court established four conditions on compulsory inoculations:
  – Must be a public health necessity
  – Must be reasonable means
  – Must not discriminate
  – Must not pose a serious health risk to the individual
• **Zucht v. King**
  – U.S. Supreme Court, 1927
  – Ruled it is within the state’s police power to require compulsory vaccination
  – Does not violate 14th Amendment

• **Court’s view of Protection Board**
  – Jenkins v. Board of Education: Contingent upon statute that specifically conveys authority
  – Freeman v. Zimmerman: Contingent upon legislature intending to confer authority
  – State of Arkansas v. Martin: Well within the board’s authority to compel vaccinations
Simple Computer Inoculation
(Analysis)

• Internet access a right?
• History
  – State-enacted computer laws:
    • Utah’s 2003 SPYWARE bill—violated the Commerce Clause
  – Federal government does have the ability to regulate interstate commerce
    • Bills have been introduced, but none enacted
    • Spy Act, Internet Spy Act, Spy-Block Act
  • Caveat: U.S. Safe Web Act of 2006—enables FTC to work with foreign governments to deter spam originating in foreign countries
Simple Computer Inoculation (Conclusion)

- Assuming, of course, that the importance of cyberspace health to society is considered to approach that of public health
- Requiring Internet-connected devices to be inoculated would not violate the Fourteenth Amendment
- Fundamental purpose of the board is valid
- Interstate commerce should not be an issue

Mass computer inoculations would fall within the limits of a state's police powers
Computer Inoculation With Feedback
(Scenario #2)

- Builds on Simple Computer Inoculation
- Incorporates a monitoring and reporting feature into the “vaccine”
- Vaccination centers insert trusted software
- Initiate ring inoculations when alerted

Seeks to detect malware and inoculate in real-time to strengthen herd immunity
Computer Inoculation With Feedback (Analysis)

- Disease surveillance & reporting are performed routinely in public health
- Every state requires health professionals to report certain infectious diseases
- No direct analog to tracking health conditions by inserting sensors in general public
- Windows Genuine Advantage—“phones home” w/o user consent
• Critical issue of PRIVACY
• U.S. Constitution does not expressly grant a right of privacy
• Griswold v. Connecticut
  – U.S. Supreme Court, 1965
  – Established “zone of privacy”
• Whalen v. Roe
  – U.S. Supreme Court, 1977
  – Private medical information can be provided to representatives of the state without violating privacy
• Abuse
  – “Human history teaches that even the loftiest of goals, such as public health protection, can always be and often are abused.”– Parmet
  – It is vital that the law stipulate that information gathered by the sensors not be used as evidence of wrongdoing
  – The law should levy severe penalties to deter abuse.

Installing sensors in computers, most likely, would NOT violate the zone of privacy
Controlled Immunized Network (Scenario #3)

- Under normal conditions works just like Computer Inoculation With Feedback
- In times of crisis:
  - Prevent computers from being enslaved
  - Quarantine infected computers
  - Support attack mitigation and recovery activities
  - Perform forensic analysis

During crisis situations (large-scale cyber attack on the critical infrastructure) the computer vaccination center serves as a “master” of a “benevolent botnet.”
• Assuming large-scale cyber attack on the critical infrastructure, these issues must be addressed:
  – Quarantine
  – Compulsory treatment
  – Controlling Authority

• Quarantine
  – Barmore v. Robertson
  – “It is NOT necessary that one be actually sick…the health authorities have the right to restrain liberties by quarantine regulations”
• Compulsory Treatment
  – A compelling interest for the intervention
  – A close connection between the means and ends
  – The intervention is the least restrictive alternative
  – Provide rigorous procedural safeguards
  – McFall v. Shrimp

• Controlling Authority
  – Government has the power of eminent domain
  – Green Dam Youth Escort
  – Inducting a personal computer in a benevolent botnet in a crisis situation is similar to a military draft or even deploying the National Guard
• The Constitution safeguards individual interests in liberty, privacy and property
• The use of controlled immunized networks must be vital and nondiscriminatory, and the least restrictive

Legal precedents would appear to support the use of controlled immunized networks
Politics – NOT Constitutionality – will determine if government-mandated computer inoculations become reality