From Target Marketing to Total Surveillance:

A Survey of Orwellian Technologies

Introduction

- Psst. This will not be an impartial evaluation.
- Here are my assumptions:
  - ID requirements are totally ineffective
    - “Improving them” will only make things worse
  - Profiling cannot catch “bad guys”
    - In fact, it creates and enables them
  - Massive data collection is questionable
  - Government purchase of this data is barely legal
  - We are facing a very dangerous future
- Adjust your bias filters, opinion lurks within (as always)
- That said, the following information is entirely factual
  - (To the best of my knowledge)

Nothing to Hide

- 4 years ago posted to membership-l about USAPA I
  - Most common response: “I have nothing to hide”
- So lets do a survey. How many people:
  - Think they have nothing to hide?
  - Think this is a good reason for total surveillance?
  - Take medication for depression or any other chronic condition?
  - Have a family history of diabetes, cancer or mental illness?
  - Are atheist or non-Christian?
  - Are not on good terms with parents/relatives?
  - How many dates do you go on/month? Sex?
  - Would like to describe what they do every day?

“Of course I don’t want to tell YOU”

- We make sure that those who have the data are trusted, right?
  - Only if being rich or well connected is our metric of trust.
  - All of this information is currently available to anyone with enough money to buy it
  - Or with a friend/relative in:
    - Law Enforcement, Marketing, Insurance, Transportation, Private Investigation, Banking/Credit/Financing
    - Furthermore, data aggregators now provide $40 software that can perform background checks
    - Not to mention crackers/carders..
- In short: A whole lot of people.

“To make an omelet…”

- Probable cause exists for a reason
- The law can be and is used as a weapon
  - Police in Canada attempted to frame journalist for exposing ineffectiveness of traffic cameras
    - Used database to determine his favorite bar
    - Attempted to frame him with a DUI
  - Enemies, jealous ex-lovers, etc.
  - MLK persecution
  - The Drug War’s use by FBI during 60s
- Following the letter of the law is impossible
  - Large potential for abuse
  - Imagine the full details of your life being available to the cop at a traffic stop. In Utah. This is happening.
- The Surveillance State is a danger to itself

The War on Anonymity

- Heavy handed regulation opens markets for defeating it
- ID requirements encourage ID forgery and theft
  - Data aggregation makes this easier
  - Criminals are undetectable, yet innocents profiled
- Possible Future Scenario:
  - “Get tough” on ID (Example: REAL ID)
    - Creates national market for fraudulent/stolen ID
      - To stop this: Mandatory biometrics/DNA DB
        - » Criminals and innocents alike begin operating through hired proxy to avoid total surveillance. Large-scale criminals can afford this. It’s just margin/operating costs.
        - » Result? Wasted tax $. No real surveillance. Many non-violent people in prison.

The Law

INFORMATION AWARENESS OFFICE
DARPA
SCIENTIA EST POTENTIA

We fought the Law...

- It turns out McCarthyism is a Bad Idea...
- Privacy Act of 1974
  - Enacted because of rampant government abuse against political opposition
    - FBI was abusing electronic search and seizure to conduct smear campaigns (Cointelpro)
- 4th Amendment interpreted to include communications.
- Electronic Communications Privacy Act of 1986
  - Protected digital communication from warrantless search
- Anti-Terrorism Act of 1996
  - Much of it was ruled unconstitutional and ineffective

And the Law Won.

- In 1990, Bush I removed restrictions on selling financial information.
- The Gramm-Leach-Bliley Act of 1999
  - Touted as financial privacy legislation
  - Made it easier to exchange/sell data
- CALEA
  - Being extended to mandate Internet surveillance equipment at ISPs/the Backbone
- E911 and FCC mandates
  - GPS data is not protected information
  - Most Phones transmit at all times
- REAL ID
  - Snuck in to military spending approvals

Patriot I

- Recently renewed
- Section 215
  - Eliminates Probable Cause for obtaining personal info
    - Medical and Psychiatric Records
    - Magazine and book purchasing
    - Membership lists of organizations
    - Library usage data
- Sect 505+Int Auth Act 374: National Security Letters
  - Recipient cannot disclose
  - Zero oversight, let alone probable cause
  - Can demand just about any data
  - Used extensively (6 pages of names in 1st 1.5 yrs)

Patriot I - cont’d

- Section 216
  - “Pen register” taps on internet/phone communications
    - No probable cause required
- Section 326 - “Know your Customer”
  - Financial institutions are required to take ID and check against “watch lists”
    - Also Jewlers, pawn brokers, car dealerships
  - Encourages ID theft and creates market for forgery
  - Does not catch criminals

Court Decisions

- Privacy policies are not contracts (Northwest)
  - Can also be changed at any time
  - “Governed” by the FTC, but can still be misleading
- You do not own your name
  - Ram Avrahami vs US News
    - Virginia: “Illegal to distribute names w/o consent”
    - Dismissed on technicality: His name was misspelled.
- No legislation protects location data
  - Currently being argued if 4th Amendment applies

Outdoing the Stasi

- Stasi were the East German Secret Police
- Most pervasive secret police force in history.
  - 1:50 informant:population ratio
- The goal of the TIPS informant program was 1:24
- TIPS was canceled in name, but lives on in many forms
  - Up until last month, tips.fbi.gov still took tips
  - Marine, highway, and community watch programs still exist and collect tips
  - Military involved also
    - Airforce Project Eagle Eyes
  - All tips are stored and cross-referenced in federal, state, and local databases

Recent Victories

- TIPS
  - As mentioned above, cancelled in name only
- IAO TIA
  - Goal was to build a complete profile on everyone
  - Dismantled by Congress. Funding cut.
- MATRIX
  - Massive inter-state information exchange system
  - Canceled, may live on through REAL ID
- States are passing anti-Patriot Act legislation
  - California: Undocumented motorists way up

Lobbying and Revolving Doors

- Data aggregation firms lobbied heavily after Sept 11th
  - Acxiom
    - $380,000 to Wesley Clark for 9/11 contracts
    - Pushed for greater access to DMV and credit info
  - ChoicePoint
    - Increased lobbying 4X to $400,000/yr after 9/11
  - TIA was proposed by Syntek
    - VP John Poindexter appointed head of the IAO
  - MATRIX system proposed by Seisint in Florida
  - National ID and database lobbying by Larry Ellison
    - (Turned out to be drunken boasting)
  - 569 other registered “homeland security” lobbyists

Implemented Technology

INFORMATION AWARENESS • OFFICE
DARPA
SCIENTIA EST POTENTIA

Data Aggregation

- Major data aggregators digitize govt records, purchase data from schools, banks, and credit card companies.
  - ChoicePoint, Experian, LexusNexus, Axciom
  - Makes ID theft both easy and dangerous
- Abacus Direct
  - “Confidential Alliance” of contributor’s data sources
    - The contributors are confidential, not your data!
    - Effectively says: “You need not worry about that pesky privacy policy”
- “Medical Information Bureau”
  - Hospitals and caregivers prevented from revealing info by HIPAA (to commercial interests, FBI is a-ok)
    - Collect info from CC and bank statements instead! Sell it to insurance companies.

Government Databases

- Federal Dept of Education
  - Maintains years worth of records on everyone
  - Can be searched without probable cause
- Pentagon Database of Children 16-25
  - Used primarily for military recruiting
- CIA’s Quantum Leap
- Able Danger
  - Allegedly uses face recognition to correlate “suspicious persons”
- Project Talon
  - Pentagon database of reports

Surveillance Industrial Complex

- Despite all this bad news, it is still illegal for the government to maintain information on individuals not suspected of any crime.
- Solution: Let the private sector do it, then buy what is needed off of them
  - DOIJ has $8m contract with ChoicePoint
  - ChoicePoint has 35 other gov't contracts
  - No audit trails on government access
    - Seisint Board member had ties to drug smugglers
  - "Voluntary Request" provides oodles of free data from corporations seeking favors
- Some police depts now provide PDA devices with access to private sector DBs

Watch Lists

- Project Lookout
  - Original FBI watch list
  - 1000 Entries
  - Circulated entirely out of control
- Watch lists are now bloated to the point of uselessness
  - Between 5-13 million names, including ex-cons and “suspicious” persons used at border
- Financial institutions must check applicants against lists
  - More incentive for ID theft

Watch List Problems

- No due process
- Negative bureaucratic incentive to remove names
  - Hard to justify removal. No one wants blame
  - Easy to justify leaving names. “Just being safe”
- Once distributed, difficult to correct
- In some areas, police officers have access to this data at the scene
- 80% of employers already perform background checks w/ data aggregators. Unknown what % use watch lists.
- Powerful tools for political persecution
  - First No Fly List contained major 3rd party figureheads

Internet Surveillance

- Eschelon
  - Once rumored, now confirmed international surveillance net
- SpyWare
  - Gathers marketing data and more sensitive info
  - Heavily linked to SPAM
  - MediaSentry
    - RIAA Spyware that watches for “illegal” copies of music
    - Horribly flawed
- Customer profiling rampant
  - DoubleClick
  - MSN Search

Internet Surveillance

- Amazon.com
  - Able to classify with frightening accuracy the books you like
- Google - now links gmail account to cell phone #
- As mentioned above, have to take it on good faith that companies are not violating their privacy policies
  - Even if they are following them, what of “voluntary disclosure” and National Security Letters?
- Law enforcement
  - Carnivore
    - Lots of hype. Basically just email sniffer
  - Complete Session capture systems are in development

Data Mining

- Too much data, too few eyes
  - Using artificial intelligence to extract features and classify examples based on features
- Used heavily by insurance and financial companies
  - Identify “Risk factors”
  - Introduces incentives for employment discrimination
- Political profiling
  - Used in 2004 to identify supporters
  - The next election will be decided by who delivers targeted messages better
    - Ability to give people a reason to vote
  - Can be determined from buying habits, donations, volunteer group affiliation

Bonus Round

- Printers secretly encode identifying information
  - Are there really that many ransom notes?
  - Are criminals going to buy a printer with a credit card? With their credit card?
  - What of anonymous whistle blowers?
  - What of pamphleteers?

Potential Technology

Profiting from Oppression

- Anyone interested in potential Orwellian technologies needs to look no further than China.
- Instead of bringing democracy, unrestrained corporate greed has caused technical progress to bring totalitarian oppression.
- Police state built and maintained by numerous US companies. 100% moral (and legal) bankruptcy.
- Foreign Relations Authorization Act of 1990
  - Assisting censorship is legal, assisting police is not.
  - Cisco engaged in PR/Disinformation campaign
- Many of these companies turn around and lobby for use of their technology for National Security
  - Cisco and Nortel proposed building a Great Firewall in the US shortly after Sept 11th

Will the Invisible Hand Please Stand Up?

- Cisco
  - Built Great Firewall at discount to corner router market
  - Video and telephone surveillance networks
  - Shockingly invasive police database (Policenet)
    - Buying habits and physical location history
    - Net access history, web posts and email
- Nortel
  - Developed network traffic analysis system dedicated to catching political opposition (Falun Gong)
- Motorola
  - Provided encrypted data network to police
  - Competed with Nokia to provide location tracking

Increasing Shareholder Value

- Sun Microsystems
  - Developed national fingerprint database
  - “Facecatch” - National face recognition system
- Nortel, Netfront, RSA Security, WatchGuard
  - Provided surveillance infrastructure
- Microsoft
  - Censors words in blog software (eg: “democracy”)
- Yahoo
  - Actively collaborates in tracking state political opponents via their email, search and chat usage
- Google
  - Censors prohibited sites/queries from search
  - Alters news results to favor nationalized news

Biometrics

- Real Time Face Recognition
  - Too inaccurate for security surveillance, just fine for marketing
  - Shared databases of avatars
  - Where did you go today?
- DNA database initiatives gaining momentum
  - Already maintain DNA of convicted criminals
  - Bills being tossed around to move this to anyone ever arrested
  - States are free to implement own laws
- Low cost DNA gatherers/classifiers are in development
- Genetic Profiling
  - Employment and insurance discrimination

Location Data Mining

- RFID
  - Passports, consumer goods, REAL ID, I-Pass
  - “What have you got in your wallet?” or your car?
- E911
  - Already under abuse by DOJ/FBI
  - Data unprotected for collection by data aggregators. This data is immensely valuable
    - What stores did you visit today? You used cash? No problem!
- OnStar/Vehicle Emergency Systems+GPS
  - Ruled illegal to monitor only because it disables use
    - This is only a technical hurdle..
  - Again, GPS data is legally unprotected

Internet Surveillance

- Ability to capture and replay specific IP sessions
- Long term classification of email is extremely valuable
  - Google might not do it now, but what happens if Yahoo makes a killing. Google is a public company. Do the shareholders care about their motto?
- Likewise with competition between the IM networks
- Widely distributed IP to Street Address mapping
  - DoubleClick intended to build, then backed down
  - Better ad targeting
  - Surfing habits can be universally indexed

Wrap Up

INFORMATION AWARENESS • OFFICE
DARPA
SCIENTIA EST POTENTIA

What can be done?

- Do not work on projects used to further the surveillance state
  - Report such projects at your workplace
  - Be aware of your company’s motives
- Stay informed
  - Politech, EFF, EPIC, ACLU
- Inform others
- Decide if target marketing is a valuable service
  - Some think it is. Most, however, agree that gov’t purchase of this data is wrong.
- Write your representatives
  - And hope it doesn’t get you on a watch list :)

Weathering the Storm

- The Achilles heal of most data aggregators is the SSN
  - This is PRIMARY KEY
  - Protect it. Only your bank and your employer legally require it.
- Also protect address/telephone number.
  - Get a UPS box. (Not Post Office – data is sold)
  - Do not file change of address forms – also are sold.
- File cumbersome paperwork with your bank and credit card companies
  - Their goal is to make it difficult
- Do not write checks
- See “How to be Invisible” by JJ Luna for more info.