The Electronic Police State

2008 National Rankings

Most of us are aware that our governments monitor nearly every form of electronic communication. We are also aware of private companies doing the same. This strikes most of us as slightly troubling, but very few of us say or do much about it. There are two primary reasons for this:

1. We really don't see how it is going to hurt us. Mass surveillance is certainly a new, odd, and perhaps an ominous thing, but we just don't see a complete picture or a smoking gun.
2. We are constantly surrounded with messages that say, "Only crazy people complain about the government."

However, the biggest obstacle to our understanding is this:

The usual image of a "police state" includes secret police dragging people out of their homes at night, with scenes out of Nazi Germany or Stalin's USSR. The problem with these images is that they are horribly outdated. That's how things worked during your grandfather's war – that is not how things work now.

An electronic police state is quiet, even unseen. All of its legal actions are supported by abundant evidence. It looks pristine.

An electronic police state is characterized by this:

State use of electronic technologies to record, organize, search and distribute forensic evidence against its citizens.

The two crucial facts about the information gathered under an electronic police state are these:

1. It is criminal evidence, ready for use in a trial.
2. It is gathered universally and silently, and only later organized for use in prosecutions.

In an Electronic Police State, every surveillance camera recording, every email you send, every Internet site you surf, every post you make, every check you write, every credit card swipe, every cell phone ping… are all criminal evidence, and they are held in searchable databases, for a long, long time. Whoever holds this evidence can make you look very, very bad whenever they care enough to do so. You can be prosecuted whenever they feel like it – the evidence is already in their database.

Perhaps you trust that your ruler will only use his evidence archives to hurt bad people. Will you also trust his successor? Do you also trust all of his subordinates, every government worker and every policeman?

And, if some leader behaves badly, will you really stand up to oppose him or her? Would you still do it if he had all the emails you sent when you were depressed? Or if she has records of every porn site you've ever surfed? Or if he knows every phone call you've ever made? Or if she knows everyone you've ever sent money to? Such a person would have all of this and more – in the form of court-ready evidence – sitting in a database, waiting to be organized at the touch of a button.

This system hasn't yet reached its full shape, but all of the basics are in place and it is not far from complete in some places. It is too late to prevent this – it is here. Our purpose in producing this report is to let people know that their liberty is in jeopardy and to help them understand how it is being undermined.

OUR RANKINGS

Firstly, we are **not** measuring government censorship of Internet traffic or police abuses, as legitimate as these issues may be. And, we are not including evidence gathering by traditional, honest police work in any of the categories below. (That is, searches pursuant to honestly obtained warrants – issued by an independent judge, and only after the careful examination of evidence.)

The seventeen factors we included in these rankings are:

Daily Documents
Requirement of state-issued identity documents and registration.

Border Issues
Inspections at borders, searching computers, demanding decryption of data.

Financial Tracking
State's ability to search and record all financial transactions: Checks, credit card use, wires, etc.

Gag Orders
Criminal penalties if you tell someone the state is searching their records.

Anti-Crypto Laws
Outlawing or restricting cryptography.

Constitutional Protection
A lack of constitutional protections for the individual, or the overriding of such protections.

Data Storage Ability
The ability of the state to store the data they gather.

Data Search Ability
The ability to search the data they gather.

ISP Data Retention
States forcing Internet Service Providers to save detailed records of all their customers' Internet usage.

Telephone Data Retention
States forcing telephone companies to record and save records of all their customers' telephone usage.

Cell Phone Records
States forcing cellular telephone companies to record and save records of all their customers' usage.

Medical records
States demanding records from all medical service providers and retaining the same.

Enforcement Ability
The state's ability to use overwhelming force (exemplified by SWAT Teams) to seize anyone they want, whenever they want.

Habeus Corpus
Lack of habeus corpus – the right not to be held in jail without prompt due process. Or, the overriding of such protections.

Police-Intel Barrier
The lack of a barrier between police organizations and intelligence organizations. Or, the overriding of such barriers.

Covert Hacking
State operatives removing – or adding! – digital evidence to/from private computers covertly. Covert hacking can make anyone appear as any kind of criminal desired.

Loose Warrants
Warrants issued without careful examination of police statements and other justifications by a truly independent judge.

For each of these, we assigned a value of between 1 and 5. A value of 1 indicates minimal development of electronic police state abilities in that area. 5 indicates a full operation.

THIS YEAR'S RESULTS

Our rankings for the year of 2008 show China and North Korea occupying the top spots as the most complete Electronic Police States in the world, followed by Belarus and Russia. Next, however, we leave communist and recently-communist states, with the UK (England/Wales), the United States and Singapore following closely on their heels.

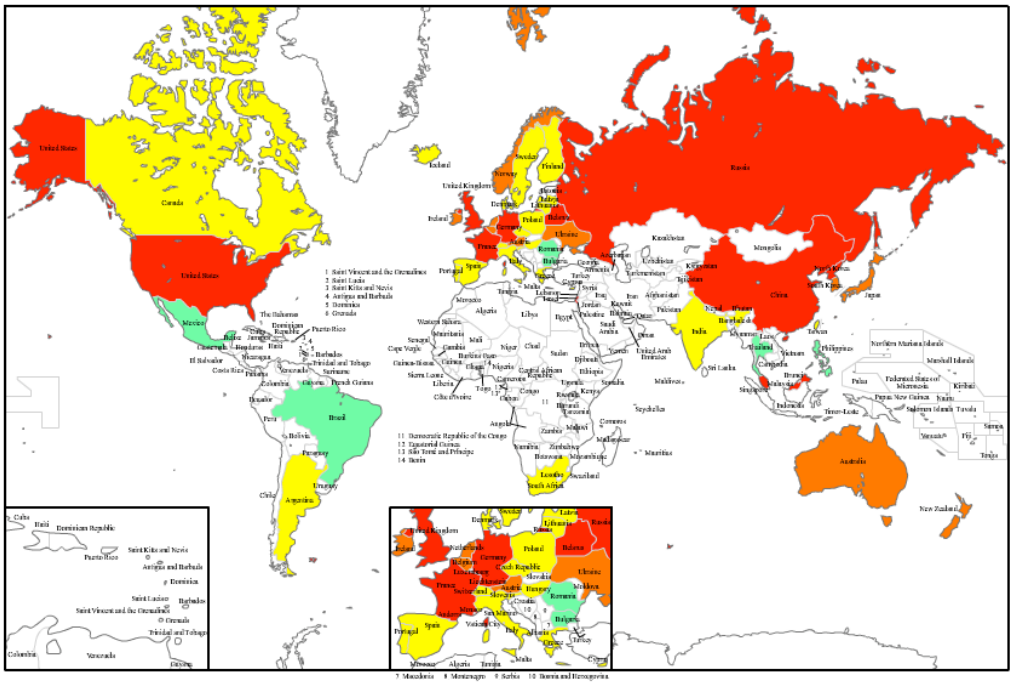
We ranked 52 major states. The map below displays their rankings:

Nations depicted in Red are the most advanced electronic police states, with an average rank of 3.0 or greater.

Nations depicted in Orange are strongly developing electronic police states, with an average rank of 2.5 or greater.

Nations depicted in Yellow are lagging (but still developing) electronic police states, with an average rank of 2.0 or greater.

Nations depicted in green are states that seem to be going toward the electronic police state model, but not as quickly.



Our raw data may be downloaded here.

Here are the 52 states and their rankings:

1. China
2. North Korea

3. Belarus
4. Russia
5. United Kingdom: England & Wales
6. United States of America
7. Singapore
8. Israel
9. France
10. Germany
11. Malaysia
12. Ireland
13. United Kingdom: Scotland
14. Netherlands
15. South Korea
16. Ukraine
17. Belgium
18. Australia
19. Japan
20. New Zealand
21. Austria
22. Norway
23. India
24. Italy
25. Taiwan
26. Denmark
27. Hungary
28. Greece
29. Canada
30. Switzerland
31. Slovenia
32. Poland
33. Finland
34. Sweden
35. Latvia
36. Lithuania
37. Cyprus

38.Malta
39.Estonia
40.Czech Republic
41.Iceland
42.South Africa
43.Spain
44.Portugal
45.Luxembourg
46.Argentina
47.Romania
48.Thailand
49.Bulgaria
50.Brazil
51.Mexico
52.Philippines

THE 2009 REPORT

We will issue next year's report toward the end of Q1. We welcome input from any and all reliable sources. (The information required to prepare such a report is not easy to obtain, and we'll take whatever help we can get.)

We may be reached at: info@cryptohippie.com