

Surveillance Art Presentation®

Alan J. Rosenthal

Prepared for:
W. Benjamin Myers, Ph.D.
Assistant Professor of Speech
University of South Carolina Upstate
Fall, 2010

Historical Glimpses of Surveillance

Referenced articles are abridged. See links for full articles.

Biblical Spies

Matthew Chapter 26, Verses 14-16 and 47-50, NASB

Then one of the twelve, named Judas Iscariot, went to the chief priests and said, "What are you willing to give me to betray Him to you?" And they weighed out thirty pieces of silver to him. From then on he *began* looking for a good opportunity to betray Jesus.

While He was still speaking, behold, Judas, one of the twelve, came up accompanied by a large crowd with swords and clubs, *who came* from the chief priests and elders of the people. Now he who was betraying Him gave them a sign, saying, "Whomever I kiss, He is the one; seize Him." Immediately Judas went to Jesus and said, "Hail, Rabbi!" and kissed Him. And Jesus said to him, "Friend, *do* what you have come for." Then they came and laid hands on Jesus and seized Him.

Stories from the History of U.S. Government Surveillance



www.trackedinamerica.org

This documentary Web site explores more than two centuries of surveillance in America. Included are two hours of audio interviews, 300 photographs, and 25 personal stories beginning in 1917. The site is designed for you to choose your path of exploration. Suggested paths include a chronological journey by time or a thematic approach following similar experiences across time.

Visitors are encouraged to get involved, submit comments to the Speak Up page, and sign up for timely updates on the issue of surveillance.

<http://www.trackedinamerica.org/download/docs/Profiles.pdf>

Alan J. Rosenthal, an Asheville, NC resident, is a former private investigator and process server with thirty-five years of experience assisting litigants and victims and over two decades in transportation. Alan is an Investigative and Personal Privacy Consultant. He is also a residential and commercial Realtor. Alan teaches Realtor® Safety at the Land of the Sky Association of REALTORS®. Please call to book consulting appointments and speaking engagements.

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Current Events-International Spies

FBI Takes Russian Spies in Custody

By Ranjan Bhaduri

Washington, June 29, (THAINDIAN NEWS) The Federal Bureau Of Investigation cracked an alleged Russian spy team in a decade long mission in United States.

Reportedly, the spy ring happens to be the biggest spy circle in America after the fall of Communist power and the charge sheet filed against them would certainly remind one of Hollywood thrillers.

FBI officials said that the Russian intelligence service, "SVR" had deployed 10 spies who landed up on the American soil years ago and gradually procured their citizenship. The idea was to get these people Americanized so that they can gather information from within without anyone suspecting them. As a matter of fact, a couple of them lived in the country as married couples to avoid any hassle or hindrance in their operations. FBI followed a trail on them and successfully intercepted the messages from SVR. The intercepted message said that the spies were sent to America in order to develop ties with the "policy making circles" in the American nation and gather intel on the same. Following that all intel were to be passed over to the Russian Command Center.

FBI special agent Amit Kachhia-Patel told the media that these arrests are an outcome of the FBI investigation in the United States which have been going on for over years. They ran a check upon all United States-based agents which finally made them aware of the existence of the foreign intelligence organ of Russia.

http://www.thaindian.com/newsportal/world/fbi-takes-russian-spies-in-custody_100387935.html

Current Events-Local Spies

Police Can Put A GPS Device On Your Car Without Your Consent

Court Reaffirms Decision That Rights Weren't Violated

<http://autos.aol.com/article/police-can-track-car-via-gps>

In case you don't have your Bill of Rights handy, here's the Fourth Amendment to the U.S. Constitution:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Ninth Circuit Court of Appeals ruled that Pineda-Moreno didn't have any signage or barriers around his property to clearly indicate that it was private property, and since "an individual going up to the house to deliver the newspaper or to visit someone would have to go through the driveway to get to the house," why couldn't the DEA? Further, the court ruled that the underside of his car isn't private because "[t]he undercarriage is part of the car's exterior, and as such, is not afforded a reasonable expectation of privacy

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Current Events-State Government Spies

'Deeply embarrassed' Pa. governor shuts down intelligence reports on peaceful protesters

By: MARC LEVY Associated Press, 09/14/10 9:10 PM EDT
<http://www.washingtonexaminer.com/nation/102897534.html>

HARRISBURG, PA. — An embarrassed Gov. Ed Rendell apologized Tuesday to groups whose peaceful protests or events, from an animal rights demonstration to a gay and lesbian festival, were the subject of regular anti-terrorism bulletins being distributed by his homeland security director. Rendell said that the information was useless to law enforcement agencies and that distributing it was tantamount to trampling on constitutional rights. Bulletins also went to members of Pennsylvania's booming natural gas industry because of several acts of vandalism at drilling sites.

Rendell said he was "deeply embarrassed," and said the fact that the state was paying for such rudimentary information was "stunning." Rendell said he ordered an end to the \$125,000 contract with the Philadelphia-based organization, the Institute of Terrorism Research and Response, that supplied the information, but said he was not firing his homeland security director, James Powers.

Aside from the drilling-related events, the bulletin mentioned other potential security concerns that it said could involve "anarchists and Black Power radicals." It listed demonstrations by anti-war groups, deportation protesters in Philadelphia, mountaintop removal mining protesters in West Virginia and an animal rights protest at a Montgomery County rodeo. It also included "Burn the Confederate Flag Day," the Jewish high holidays and the Muslim holy month of Ramadan as potential sources of risk. The bulletins, which went out three times a week, were not intended for public distribution.

Forty years later, we are no further along when it comes to civil rights and freedom from governmental surveillance and its assault on the privacy of citizens.

From Tracked in America

J. Edgar Hoover, director of the FBI for almost 50 years, was given free reign to pursue civil rights activists based on his suspicion that communists were infiltrating civil rights organizations to overthrow the government. Hoover sent informants to church meetings, intercepted mail and phone calls, engineered break-ins, and planted news stories to defame civil rights leaders. COINTELPRO (Counter Intelligence Programs) was also instituted against the Communist Party, Socialist Workers Party, white supremacists, black nationalists, and the New Left. Although the civil rights movement ultimately succeeded, many lives were harmed in the process.

Many young people who began their political activism during this time transferred their commitment to social justice to other causes, including protests against the Vietnam War in the late 1960s and '70s. The government's suppression of anti-war protestors and civil rights activists was framed as a fight against the spread of communism, so those who opposed the Vietnam war were often accused of sympathizing with the enemy. In addition to surveillance by the FBI and local authorities, the U.S. Army also began secretly and illegally monitoring protests and anti-war groups. The Army's activities were stopped in 1971, after being exposed by a Senate subcommittee chaired by Sam Ervin Jr., a conservative Democrat from North Carolina.

<http://www.trackedinamerica.org/download/docs/Profiles.pdf>, Page 5.

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Interpersonal Spies



If this type of software can be remotely installed on your computer without your knowledge or permission, can you ever be safe when online?

The World's Best-Selling Monitoring Software

Spector Pro has deservedly earned its reputation as not only the most trusted monitoring software in the world, but as also the most feature-rich, while being easy and intuitive... even for beginners! With the world's best Screen Snapshot Surveillance recorder, you can see EVERYTHING they do, in the EXACT order they do it, Step-by-Step.

Capture Keystrokes Typed
Capture Chats and IM's
Capture Emails
Capture Sites Visited
Remote Viewer

Capture Searches
Capture Program Activity
Capture Keyword Activity
Website and Chat Blocking
Screen Capture

[A Few Stories from Alan's Case Files](#)

A cheating and abusive husband placed a "keylogger" program on his wife's computer. This program recorded all of her email and internet usage. When she needed to go to an abuse shelter, he knew where she went as he read the emails between his victim, her lawyer and her investigator. I found this hidden program and was able to stop the spying and show the victim the years of stolen emails and tracking. I also was successful in having the software company that sold the program change its marketing to protect victims of abuse.

A woman was being stalked online by a man she met in a chat room. By triangulating the stalker using other operatives, I was able to get the stalker to identify himself. Moments later, his phone rang. His next victim was this investigator. The victimization stopped that evening.

An elderly couple with dementia was being victimized by a home health aide who would access and change the couple's financial data, adding herself as a primary agent. By installing the proper surveillance software, I was able to track the identity theft and protect the couple's assets.

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Academic Spies-Academic Integrity & Campus Security



Photo by Alanna Tisdale

To Stop Cheats, Colleges Learn Their Trickery

By TRIP GABRIEL

ORLANDO, Fla. — The frontier in the battle to defeat student cheating may be here at the testing center of the University of Central Florida. No gum is allowed during an exam: chewing could disguise a student's speaking into a hands-free cellphone to an accomplice outside. The 228 computers that students use are recessed into desk tops so that anyone trying to photograph the screen — using, say, a pen with a hidden camera, in order to help a friend who will take the test later — is easy to spot. Scratch paper is allowed — but it is stamped with the date and must be turned in later.

When a proctor sees something suspicious, he records the student's real-time work at the computer and directs an overhead camera to zoom in, and both sets of images are burned onto a CD for evidence. Some educators have rejected [anti-cheating services] and other anti-cheating technologies on the grounds that they presume students are guilty, undermining the trust that instructors seek with students

For similar reasons, some students at the University of Central Florida objected to the business school's testing center with its eye-in-the-sky video in its early days, Dr. Ellis said. But recently during final exams after a summer semester, almost no students voiced such concerns. Rose Calixte, a senior, was told during an exam to turn her cap backward, a rule meant to prevent students from writing notes under the brim.

A first-year M.B.A. student, Ashley Haumann, said that when she was an undergraduate at the University of Florida, "everyone cheated" in her accounting class of 300 by comparing answers during quizzes. She preferred the highly monitored testing center because it "encourages you to be ready for the test because you can't turn and ask, 'What'd you get?'" As for Central Florida's testing center, one of its most recent cheating cases had nothing to do with the Internet, cellphones or anything tech. A heavily tattooed student was found with notes written on his arm. He had blended them into his body art.

<http://www.nytimes.com/2010/07/06/education/06cheat.html>

Campus Security Articles

The Eyes of [University of] Texas are Upon . . . YOU!

<http://www.notbored.org/texas.html>

Surveillance cameras on campus triple

<http://www.browndailyherald.com/campus-news/surveillance-cameras-on-campus-triple-1.1679524>

Setting the Security Bar High - With IP surveillance cameras, campuses ensure student safety — but the data amassed also spurs colleges to craft smart video storage strategies.

<http://www.edtechmag.com/higher/june-july-2010/setting-the-security-bar-high-3.html>

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Creative Resistance

- Don't give out any information.
- Do not participate in many aspects of life.
- Live in the apartment next to the police station.
- Don't register to vote, get a firearm, start a business or get a phonenumber.
- Give the wrong info but then remember your wrong info.
- Don't leave cookies for Santa or install a Nanny Cam.

Resistant Practices

Counter-surveillance as Political Intervention? By Torin Monahan
SOCIAL SEMIOTICS VOLUME 16 NUMBER 4 (DECEMBER 2006)

This paper analyzes practices of counter-surveillance* particularly against closed-circuit television systems in urban areas* and theorizes their political implications.

Counter-surveillance is defined as intentional, tactical uses, or disruptions of surveillance technologies to challenge institutional power asymmetries.

Such activities can include disabling or destroying surveillance cameras, mapping paths of least surveillance and disseminating that information over the Internet, employing video cameras to monitor sanctioned surveillance systems and their personnel, or staging public plays to draw attention to the prevalence of surveillance in society. The main argument is that current modes of activism tend to individualize surveillance problems and methods of resistance, leaving the institutions, policies, and cultural assumptions that support public surveillance relatively insulated from attack.

Conclusions

Are counter-surveillance activities political interventions? Yes, they are clearly political. The central question remains, however, as to which counter-surveillance configurations provide productive critiques and interventions. Because counter-surveillance movements, in my definition of them, seek to correct unequal distributions of power, they do destabilize status quo politics on a case-by-case basis* on the ground, at specific, temporally bounded sites of contestation. If our vantage point is once removed, however, then individualized counter-surveillance efforts appear to provide the necessary provocations for those with institutional power to diagnose and correct inefficiencies in their mechanisms of control.

Even if this second conclusion is persuasive, however, it should not imply that activists and counter-surveillance practitioners should dispense with their interventionist projects, but instead that they should diligently avoid reproducing the exclusionary logics and reactionary stances of those whom they critique. For instance, high-tech interventions may attract public attention because of their innovative use of technologies, but they can defy replication by others without comparable technical capabilities or resources. Furthermore, focusing on individual agents of surveillance (such as store clerks, security guards, camera operators, or police) artificially reduces the complexity of the problem: many of these individuals are underpaid yet completely dependent upon their jobs, so they might be easy targets, but not necessarily the best ones. The strength of social movements lies in their inclusiveness and in their participatory structures (Breyman 2001; Juris 2004). So while these attributes might signify areas of vulnerability for activists, they remain the magnets that draw people into movements and mobilize them behind causes* they are the qualities that need to be nourished for less individualistic and more effective activism to take root.

ISSN 1035-0330 print/1470-1219 online/06/040515-20 # 2006 Taylor & Francis DOI:
10.1080/10350330601019769
<http://torinmonahan.com/papers/Counter-Surveillance.pdf>

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Investigative Surveillance for the Private Investigator

This outline deals mostly with surveillance within the realm of private investigation where the information gained is most often connected to the purpose of fairness within the justice system. Fairness can not be achieved without transparency. Surveillance takes on a wholly different tone and form when it is the government watching its citizenry for political purposes or to justify a questionable or unconstitutional policy. At what point is surveillance an abuse of human rights? This outline does not seek to answer that question. Some resources are provided to assist you to delve deeper and make up your own mind about the propriety of surveillance measures.

A Simple Purpose:

Obtaining information not ascertainable by other methods.
See definitions below.

Target Types

Unaware, Suspicious, Don't Care

Some Types of Cases Requiring Surveillance

Vehicular Accidents	Domestic Abuse
Slip and Fall	Neighbor Disputes
Staged Accidents	White Collar Crime
Corporate Fraud	Homicide
Sexual Harassment	Theft
Infidelity	Premises Accidents
Child Abuse	Personal Negligence
Divorce	Workers Comp.

Some Crimes Surveillance Can Solve and Sometimes Prevent

Physical Assaults	Gambling
Sexual Assaults	Organized Crime
Robbery	Terrorism
Arson, Bombings	Theft
Hate Crimes	Hit & Run
Property Crimes	Burglary
Nanny Crimes	Carjacking
Drug Dealing	Rape
Prostitution	Child Sexual Abuse

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Types of Surveillance

Stationary Stakeouts & Moving Surveillance

Vehicular: Auto, Air, Water,

Public Transportation: Subways, Trains, Buses, Taxis

Foot

Combinations of Methods

Public Locations, Highways, Close Quarters, Small Town, Cities

Following Someone from In Front of Them

Day or Night

Visual and Audio

Dumpster Diving

Monitoring Communications

Monitoring Internet Activity

Dumpster Diving

Back Office Operations

Indispensable Resource

To be a Back Office Operator

“I’ve been made.”

It happens.

Not the end of the world, just the end of today’s surveillance.

Different car, different operative.

Unintended consequences.

Subject confesses for being tired of being watched.

Subject calls the police.

Subject attacks you.

Getting “made” on purpose.

Counter-surveillance

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Definitions

The secretive, continuous, and sometimes periodic watching of persons, vehicles, places, or objects to obtain information concerning the activities and identities of individuals. Observation of people to determine information relevant to an investigation without the subject being aware of the observation. Watching and/or following a person.
McMahon, Rory J., Practical handbook for Private Investigators (2001)

The covert observation of a person, place or situation from concealment for a specific purpose. From the French *surveiller*, “to watch over”.
MacHovec, Ph.D., Frank, Private Investigation (1991)

Physical surveillance is the systematic, discreet observation of an individual to develop information regarding his activities.
ACM IV Security Services, Secrets of Surveillance: A Professional’s Guide to Tailing Subjects by Vehicle, Airplane and Public Transportation (1993)

From the word *vigil*. Etymologically, to take part in a *vigil*, you have to be ‘alert’ and ‘awake’. The word comes via Old French *vigile* from Latin *vigilia*, which was derived from the adjective *vigil* ‘awake’ and ‘alert,’ so the notion underlying it is of staying awake to keep watch. Another derivative of the Latin adjective was *vigilare* ‘keep watch,’ which lies behind English *reveille*, *surveillance*, *vigilant* and *vigilante* (via Spanish)/
Ayto, John, Dictionary of Word Origins (1990).

Close observation of a person or group, especially one under suspicion. The act of observing or the condition of being observed.
The American Heritage Dictionary of The English Language, Third Edition (1996)

Oversight, superintendence, supervision. Police investigative technique involving visual or electronic observation or listening directed at a person or place (e.g. stakeout, tailing of suspects, wiretapping). Its objective is to gather evidence of a crime or merely to accumulate intelligence about suspected criminal activity.
Black’s Law Dictionary, Sixth Edition (1990)

Physical surveillance is nothing more than watching or observing people, places, and things. Electronic surveillance is much like physical surveillance, however the investigator enhances his capabilities using electronic technology.
Ferraro, CPP, CFE, Eugene F., Undercover Investigations in the Workplace (1999)

Important Privacy Authors and Books

Garfinkel, Simson
Database Nation – The Death of Privacy in the 21st Century (2000)

Etzioni, Amitai

ACM IV Security Services
Surveillance Countermeasures: A Serious Guide to Detecting, Evading, and Eluding Threats to Personal Privacy (1993)

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Tools of Surveillance

Proper dress

Pre surveillance data

Interviews, documents, public records, databases, etc.

Maps and foreknowledge of area

Appropriate and maintained vehicles and fuel

Communications equipment, phones, radio, text

Monitoring & Recording Equipment

Cameras

Still and Motion, Lenses, Film, Digital Cards

Microphones, Transmitters, Recorders

Stationary, Body, Bugs

Phone Monitoring Equipment

Tracking Devices

Laptop

Internet Access

Internet Monitoring Software

Writing Implements and Paper

Weapons

Lawful weapons

Proper training

Know where you're going

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

Surveillance and Privacy Links

The links found below are in no way an exhaustive set of references on surveillance and privacy. At best, they are starting points which help you to begin your journey into these very important realities of today's world. As an adept and thorough investigator who wishes to be a professional in the field, you have to understand that law, social custom, practicality and effectiveness all come together when putting together the pieces of a human puzzle.

Wiretaps and Phone Recording

http://www.justice.gov/criminal/cybercrime/wiretap2510_2522.htm

<http://www.brickhousesecurity.com/about-wire-tap-and-phone-recording-laws.html>

Privacy

! <http://epic.org/>

! <http://www.privacyfoundation.org/index.cfm>

<http://epic.org/privacy/facebook/>

<http://epic.org/privacy/>

<http://www.ftc.gov/privacy/>

<http://www.law.fsu.edu/journals/lawreview/downloads/251/overton.pdf>

Pretexting

<http://writ.news.findlaw.com/ramasastry/20060123.html>

Dumpster Diving

<http://www.rbs2.com/privacy.htm#anchor666666>

Identity Theft

<http://www.llrx.com/features/idtheftguide.htm>

Duty to Destroy

<http://www.shrednations.com/articles/Shredding-Compliance.php>

Health Information

<http://www.hhs.gov/ocr/privacy/index.html>

Family Computer

<http://www.famlawconsult.com/archive/reader200202.html>

http://ecoustics-cnet.com.com/Court+Wife+broke+law+with+spyware/2100-1030_3-5577979.html

Data Breaches

http://news.cnet.com/FAQ-Protecting-yourself-from-search-engines/2100-1025_3-6103486.html?tag=mncol;txt

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

A Short List of Privacy Related Laws

Federal Statutes

A wide range of federal laws relate to identity theft. Laws can be grouped into four main categories: Identity theft specific laws, false identification laws, privacy and personal data laws, and credit law. Identity theft specific laws are those that were designed and enacted to criminalize the act of identity theft. False Identification laws deal specifically with fraud in connection with personal identifying documents. Privacy and personal data laws can help prevent identity theft by regulating how personal identifying information (PII) is collected and disseminated. Laws regarding credit directly impact victims of identity theft, as those individuals must restore their credit ratings and limit their liability for unauthorized debts. In particular, the following statutes are frequently cited in the literature regarding identity theft.

Identity Theft Statutes

1. Identity Theft and Assumption Deterrence Act of 1998

P.L. 105-318

Enacted H.R. 4151, October 30, 1998

112 Stat. 3007, codified at 18 U.S.C § 1028

2. Identity Theft Penalty Enhancement Act

P.L. 108-275

Enacted H.R. 1731 / S.153, July 15, 2004

118 Stat. 831, Added 18 U.S.C. § 1028A

3. The Fair and Accurate Credit Transactions Act of 2003

P.L. 108-159

Enacted H.R. 2622 / S. 1753, December 4, 2003

117 Stat. 1952, U.S.C. § 1681 et seq.

False Identification Statutes

1. False Identification Crime Control Act of 1982

P.L. 97-398

H.R. 6946, December 31, 1982

96 Stat. 2009, Added 18 U.S.C § 1028 & 18 U.S.C. § 1738

2. Internet False Identification Act of 2000

P.L. 106-578

Enacted S. 2924, December 28, 2000

114 Stat. 3075, Codified at 18 U.S.C 1001, 1028

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org

Surveillance Art Presentation®

Alan J. Rosenthal

C. Statutes Governing Privacy and the Use of Personal Data

1. Privacy Act of 1971

P.L. 93-579 Enacted S.3418, December 31, 1974
88 Stat. 1896, Codified 5 U.S.C. § 552a

2. Drivers Privacy Protection Act of 1994

P.L. 103-322 (Title XXX), amended by 106-69
Enacted, as amendment to H.R. 3355, September 13, 1994
108 Stat. 2099, 18 U.S.C. §§ 2721-2725

3. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

P.L. 104-191 Enacted H.R. 3103, August 21, 1996
110 Stat. 1936, codified 42 U.S.C. 1320

4. Gramm-Leach- Bliley Act of 1999

P.L. 106-102 Enacted S. 900, November 12, 1999
113 Stat. 1338, 15 U.S.C. § 6801, et seq.

5. Social Security Number Confidentiality Act of 2000

P.L. 106-433 Enacted H.R. 3218, November 6, 2000
114 Stat. 1910, 31 U.S.C. § 3327

D. Federal Credit Laws

1. The Fair Credit Reporting Act

P.L. 91-508 (Title VI § 601) October 26, 1970
84 Stat. 1128, 15 U.S.C. § 1681 to 1681u

2. Truth in Lending Act

P.L. 90-321 (Title I § 104) May 29, 1968
82 Stat. 147, 15 U.S.C. § 1601

3. Electronic Fund Transfer Act

P.L. 95-630 (Title XX § 2001) November 10, 1978
92 Stat. 3728, 15 U.S.C. § 1693 et seq.

4. Fair Credit Billing Act

P.L. 93-495 (Title III) October 28, 1974
88 Stat. 1511, 15 U.S.C § 1666 et seq.

Additional Privacy Related Laws

Social Security Act of 1934

Privacy Act of 1974

Right to Financial Privacy Act of 1978

California v. Greenwood (1988)

The Modern Era of Privacy Protection Legislation

Economic Espionage Act of 1996.

Fair Credit Reporting Act of 2001.

Sarbanes-Oxley Act of 2002.

Fair and Accurate Credit Transactions Act of 2003 (FACTA)

The Alan J. Rosenthal Group, Inc.



850-510-6469 RosenthalConsultants@gmail.com AlanRosenthal.org