Information Technology Fundamentals

Mohammad Hossein Manshaei
manshaei@gmail.com

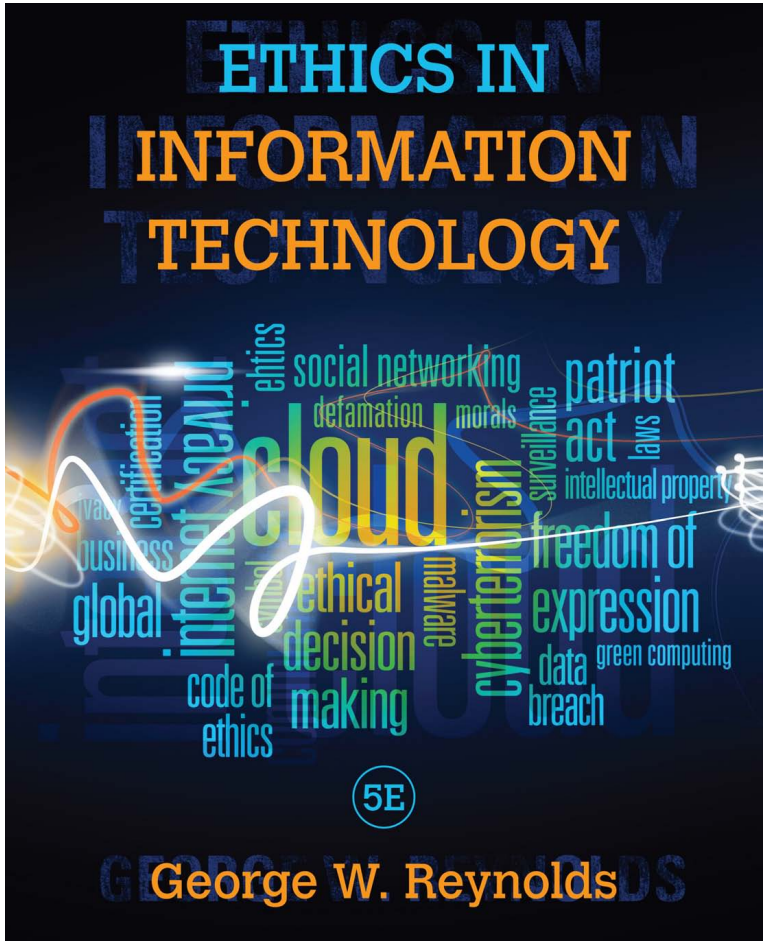
Information Assurance & Security: Electronic Surveillance
Module 7: Part 2

Module 7. Main Objectives

1. Define Main Concepts of Information Privacy
2. Review Privacy Laws, Applications, and Key issues

Main Reference

- George W. Reynolds, 2011. **Ethics in Information Technology.** Engage Learning.



Contents

- ➢Privacy Protection and the Law
  - ◇Information Privacy
  - ◇Privacy Laws, Applications, and Court Rulings
    - Financial Data
    - Health Information
    - Children Personal Data
    - Electronic Surveillance
    - Export of Personal Data and Access to Government Records

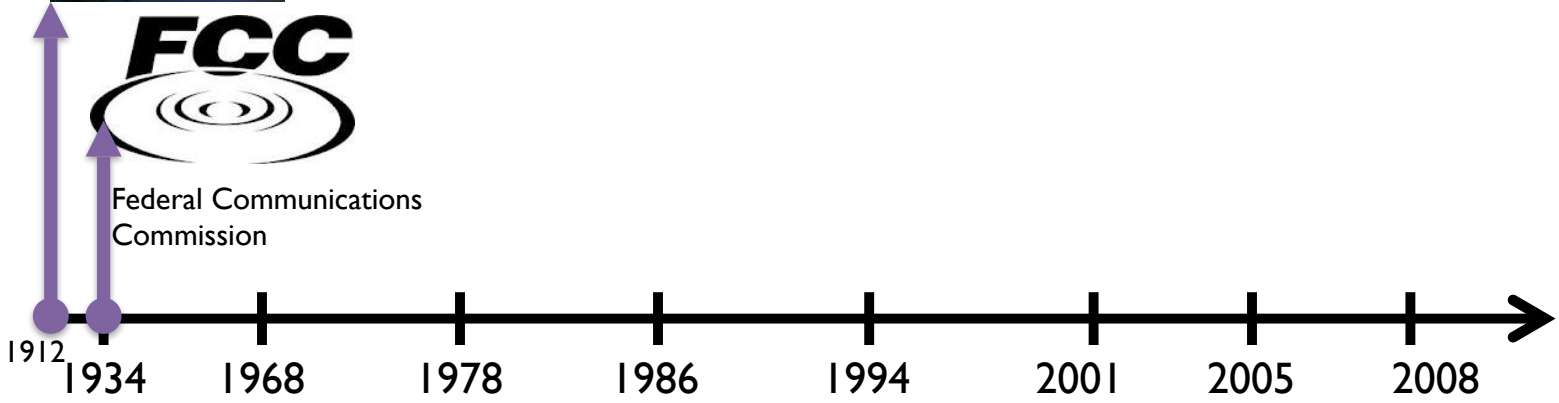
Electronic Surveillance

Government surveillance laws

New laws have been added and old laws amended:

- ➢Worldwide terrorist activities
- ➢Development of new communication technologies

History (Electronic Surveillance)



1934: Communications Act

- Established the Federal Communications Commission (FCC)
- Regulation of non-federal-government use of:
  - Radio
  - Television broadcasting
  - Interstate telecommunications—including wire, satellite, and cable
  - All international communications that originate or terminate in the United States

History (Electronic Surveillance)

Federal Communications Commission

1934 1968 1978 1986 1994 2001 2005 2008

WireTap Act

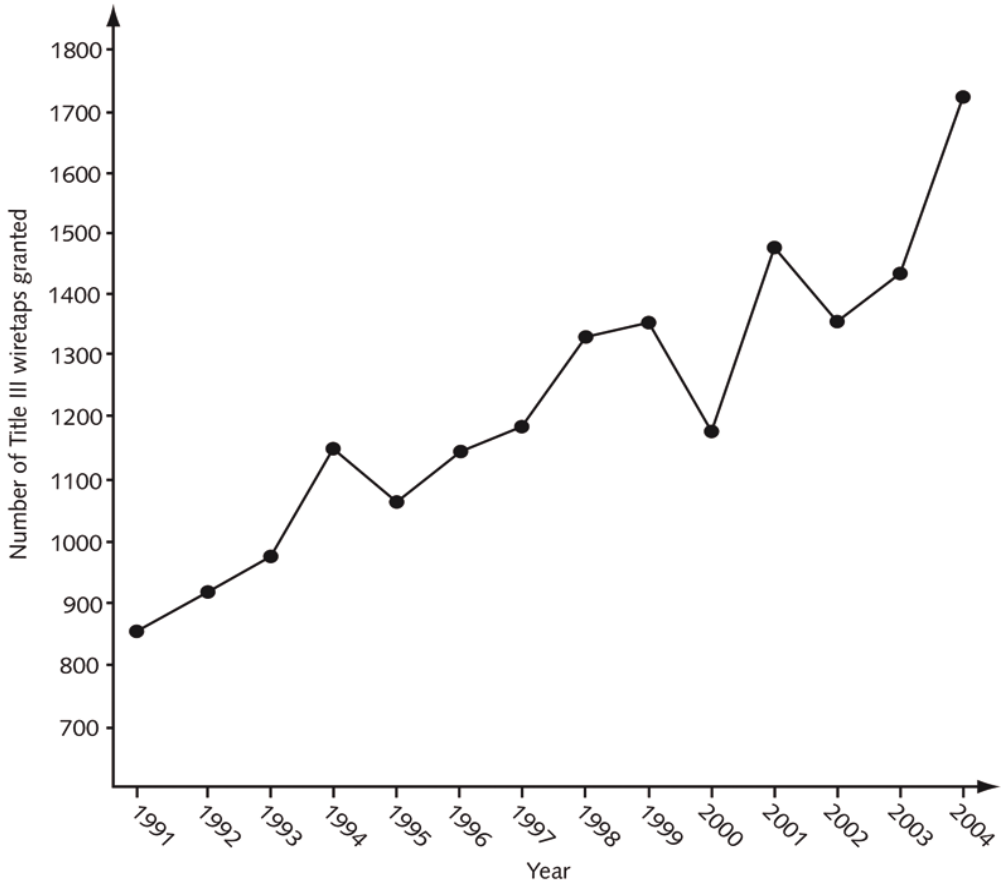
1968: Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act)

- **Federal Wiretap Act**
  - Outlines processes to obtain court authorization for surveillance of all kinds of electronic communications
  - Judge must issue a court order based on probable cause
    - Almost never deny government requests
  - "**Roving tap**" authority
    - Does not name specific telephone lines or e-mail accounts
    - All accounts are tied to a specific person

Judge Should Approve

approve the warrant only if
"there is probable cause [to believe] that an individual is committing, has committed, or is about to commit a particular offense . . . [and that] normal investigative procedures have been tried and have failed or reasonably appear to be unlikely if tried or to be too dangerous."

Number of Title III Wiretaps Granted



Source: Administrative Office of the U.S. Courts, www.uscourts.gov/wiretap.html for 1997-2004 wiretap reports.

Case: Katz vs United States

- Katz was convicted of illegal gambling
  - based on recordings of his various telephone calls made from a public phone booth (by FBI)
- Katz challenged the conviction based on a violation of his Fourth Amendment rights
- In 1967 **he won** !!
  - Court ruled that "the Government's activities in electronically listening to and recording the petitioner's words violate the privacy"

History (Electronic Surveillance)

Federal Communications Commission

Foreign Intelligence Surveillance Act (FISA)

1934 1968 1978 1986 1994 2001 2005 2008

WireTap Act

1978: Foreign Intelligence Surveillance Act (FISA)

- Allows wiretapping of aliens and citizens in the United States Based on finding of probable cause that a target is
  - Member of a foreign terrorist group
  - Agent of a foreign power
- Legal authority for electronic surveillance outside the United States

History (Electronic Surveillance)

Federal Communications Commission

Foreign Intelligence Surveillance Act (FISA)

1934 1968 1978 1986 1994 2001 2005 2008

WireTap Act

2008: Foreign Intelligence Surveillance Amendments

- Gathering foreign intelligence and implemented legal protections for electronic **communications service providers** who previously provided consumer data to the **National Security Agency (NSA)** and the **CIA**.

History (Electronic Surveillance)

Federal Communications Commission

Foreign Intelligence Surveillance Act (FISA)

1934 19 68 1978 19 86 1994 2001 2005 2008

WireTap Act

Electronic Communications Privacy Act (ECPA)

1986: Electronic Communications Privacy Act (ECPA)

- Deals with three main issues:
  1. The **protection of communications** while in transfer from sender to receiver
  2. The protection of communications **held in electronic storage**
  3. The **prohibition of devices to record** dialing, routing, addressing, and signaling information without a search warrant.

1986: Electronic Communications Privacy Act (ECPA)

- Sets standards for access to stored e-mail and other electronic communications and records
- Extends Title III's prohibitions against the unauthorized interception, disclosure, or use of a person's oral or electronic communications
- Prosecutor does not have to justify requests

1986: Electronic Communications Privacy Act (ECPA)

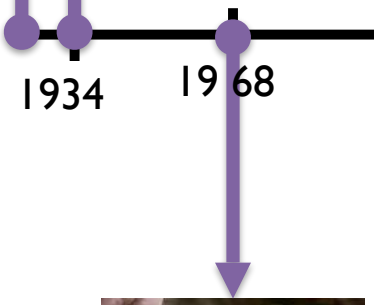
- Highly controversial
  - Especially collection of computer data sent over the Internet
- Failed to address emerging technologies

History (Electronic Surveillance)

Federal Communications Commission

Foreign Intelligence Surveillance Act (FISA)

Communications Assistance for Law Enforcement Act (CALEA)



WireTap Act

Electronic Communications Privacy Act (ECPA)

1994: Communications Assistance for Law Enforcement Act (CALEA)

- Requires the telecommunications industry to **build tools into its products** so that federal investigators **can eavesdrop** on conversations
- Contains a provision covering **radio-based data communication**
- Includes voice over Internet (**VoIP**) technology

History (Electronic Surveillance)

Federal Communications Commission

Foreign Intelligence Surveillance Act (FISA)

Communications Assistance for Law Enforcement Act (CALEA)

1934 19 68 1978 19 86 1994 2001 2005 2008

WireTap Act

Electronic Communications Privacy Act (ECPA)

USA PATRIOT

2001: USA PATRIOT Act

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

- Passed just after the terrorist attacks of September 11, 2001.
- Gives sweeping new powers to
  - Domestic law enforcement
  - International intelligence agencies
- Contains several "sunset" provisions

Key Provisions of the USA Patriot Act

201	Wiretapping in terrorism cases	Added several crimes for which federal courts may authorize wiretapping of people's communications
202	Wiretapping in computer fraud and felony abuse cases	Added computer fraud and abuse to the list of crimes the FBI may obtain a court order to investigate under Title III of the Wiretap Act
203(b)	Sharing wiretap information	Allows the FBI to disclose evidence obtained under Title III to other federal officials, including "law enforcement, intelligence, protective, immigration, national defense, [and] national security" officials
203(d)	Sharing foreign intelligence information	Provides for disclosure of threat information obtained during criminal investigations to "appropriate" federal, state, local, or foreign government officials for the purpose of responding to the threat

Key Provisions of the USA Patriot Act

204	FISA pen-register/trap-and-trace exceptions	Exempts foreign intelligence surveillance from statutory prohibitions against the use of pen-register or trap-and-trace devices, which capture "addressing" information about the sender and recipient of a communication; it also exempts the U.S. government from general prohibitions against intercepting electronic communications and allows stored voice-mail communication to be obtained by the government through a search warrant rather than more stringent wiretap orders
206	FISA roving wiretaps	Expands FISA to permit "roving wiretap" authority, which allows the FBI to intercept any communications to or by an intelligence target without specifying the telephone line, computer, or other facility to be monitored
207	Duration of FISA surveillance of non-U.S. agents of a foreign power	Extends the duration of FISA wiretap orders relating to an agent of a foreign power from 90 days to 120 days, and allows an extension in 1-year intervals instead of 90-day increments
209	Seizure of voice-mail messages pursuant to warrants	Enables the government to obtain voice-mail messages under Title III using just a search warrant rather than a wiretap order, which is more difficult to obtain; messages stored on an answering machine tape, however, remain outside the scope of this section

Key Provisions of the USA Patriot Act

212	Emergency disclosure of electronic surveillance	Permits providers of communication services (such as telephone companies and Internet service providers) to disclose consumer records to the FBI if they believe immediate danger of serious physical injury is involved; communication providers cannot be sued for such disclosure
214	FISA pen-register/trap-and-trace authority	Allows the government to obtain a pen-register/trap-and-trace device "for any investigation to gather foreign intelligence information"; it prohibits the use of FISA pen-register/trap-and-trace surveillance against a U.S. citizen when the investigation is conducted "solely on the basis of activities protected by the First Amendment"

Key Provisions of the USA Patriot Act

215	FISA access to tangible items	Permits the FBI to compel production of any record or item without showing probable cause; people served with a search warrant issued under FISA rules may not disclose, under penalty of law, the existence of the warrant or the fact that records were provided to the government. It prohibits investigation of a U.S. citizen when it is conducted solely on the basis of activities protected by the First Amendment.
217	Interception of computer-trespasser communications	Creates a new exception to Title III that permits the government to intercept the "communications of a computer trespasser" if the owner or operator of a "protected computer" authorizes it; it defines a protected computer as any computer "used in interstate or foreign commerce or communication" (because of the Internet, this effectively includes almost every computer)
218	Purpose for FISA orders	Expands the application of FISA to situations in which foreign intelligence gathering is merely a significant purpose rather than the sole purpose

Key Provisions of the USA Patriot Act

220	Nationwide service of search warrants for electronic evidence	Expands the geographic scope in which the FBI can obtain search warrants or court orders for electronic communications and customer records
223	Civil liability and discipline for privacy violations	Provides that people can sue the government for unauthorized disclosure of information obtained through surveillance
225	Provider immunity for FISA wiretap assistance	Provides immunity from lawsuits for people who disclose information to the government pursuant to a FISA wiretap order, a physical search order, or an emergency wiretap or search
505	Authorizes use of National Security Letters (NSLs) to gain access to personal records	Authorizes the attorney general or a delegate to compel holders of your personal records to turn them over to the government simply by writing a National Security Letter, which is not subject to judicial review or oversight; NSLs can be used against anyone, including U.S. citizens, even if they are not suspected of espionage or criminal activity

2005: Sunset Provision

- Section 215: Extended for four years and altered slightly so that recipient of FISA subpoenas for record searches would have the right to consult with a lawyer to challenge the request in court.

- Section 505: Modified so that the recipient of an NSL could challenge the nondisclosure requirement but no sooner than one year after receiving the National Security Letter.

Contents

- Privacy Protection and the Law
  - Information Privacy
  - Privacy Laws, Applications, and Court Rulings
    - Financial Data
    - Health Information
    - Children Personal Data
    - Electronic Surveillance
    - Export of Personal Data and Access to Government Records

Export of Personal Data

Guidelines to ensure that the flow of personal data across national boundaries does not result in:

1. The **unlawful storage** of personal data

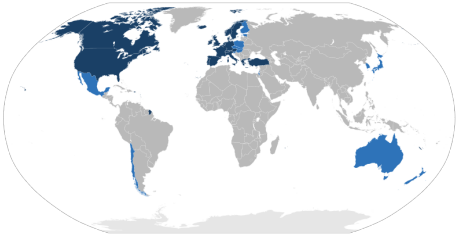
2. The storage of **inaccurate personal data**

3. The **abuse** or **unauthorized disclosure of such data**

Important Guidelines:

- Organization for Economic Co-operation and Development Fair Information Practices (OECD)

- European Union Data Protection Directive



1980: OECD

- International organization consisting of 30 member:
  - Australia, Canada, France, Germany, Italy, Japan, Mexico, New Zealand, the UK, and the US

- 1980: privacy guidelines set by OECD (known as the Fair Information Practices)

- These guidelines are composed of the **eight principles**

Summary of the 1980 OECD Privacy Guidelines

Principle	Guideline
Collection limitation	Limit the collection of personal data; all such data must be obtained lawfully and fairly with the subject's consent and knowledge
Data quality	Personal data should be accurate, complete, current, and relevant to the purpose for which it is used
Purpose specification	The purpose for which personal data is collected should be specified and should not be changed
Use limitation	Personal data should not be used beyond the specified purpose without a person's consent or by authority of law
Security safeguards	Personal data should be protected against unauthorized access, modification, or disclosure
Openness principle	Data policies should exist, and a data controller should be identified
Individual participation	People should have the right to review their data, to challenge its correctness, and to have incorrect data changed
Accountability	A data controller should be responsible for ensuring that the above principles are met

Source: Organisation for Economic Co-operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

1998: European Union Data Protection Directive

- European data privacy principles:
  - *Notice:* Tell all customers what is done with their information.
  - *Choice:* Give customers a way to opt out of marketing.
  - *Onward transfer:* Provide at least the same level of protection for data, when it is forwarded.
  - *Access:* Give customers access to their information.
  - *Security:* Protect customer information from unauthorized access.
  - *Data integrity:* Ensure that information is accurate and relevant.
  - *Enforcement:* Independently enforce the privacy policy.

Other Initiatives: BBB Online and TRUSTe

- BBB Online and TRUSTe
  - Independent, nonprofit initiatives
  - Favor an industry-regulated approach to data privacy

Better Business Bureau Online (BBBOnLine)

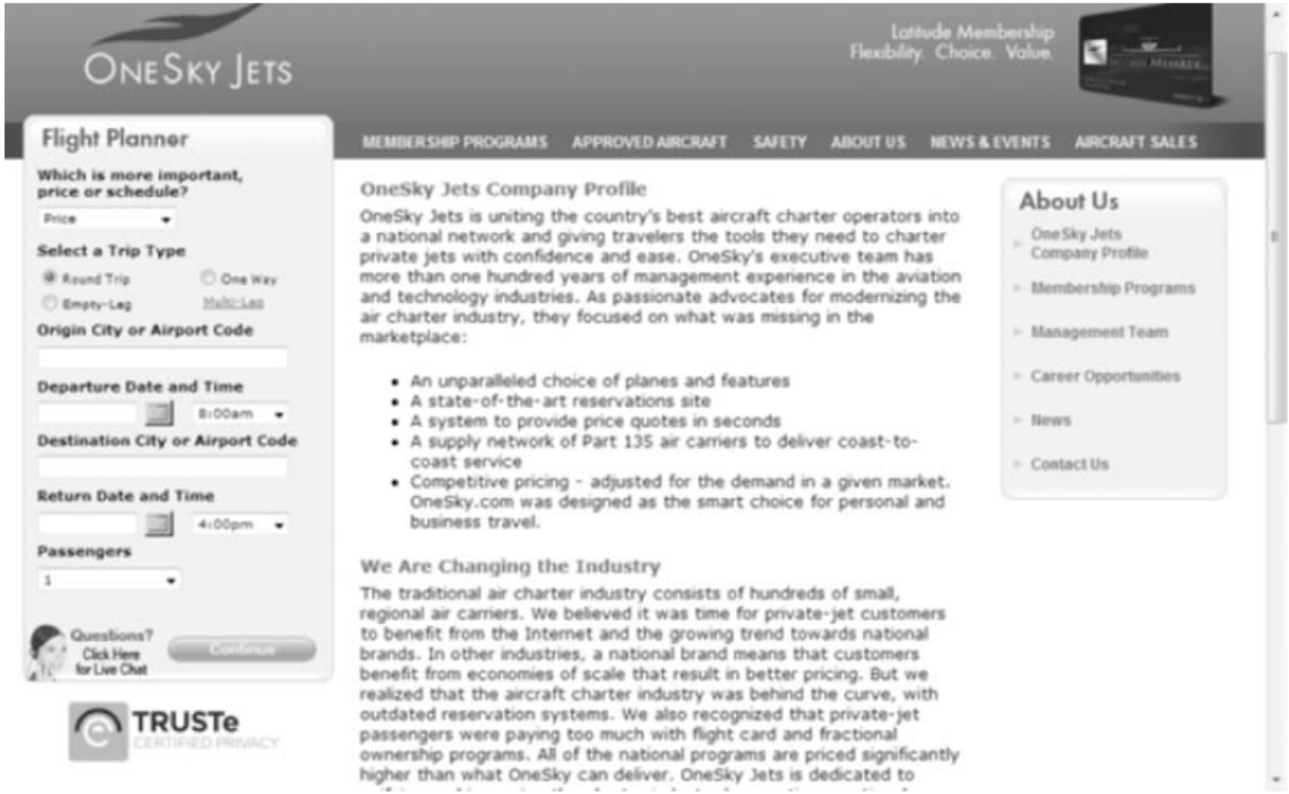
- Pay an annual fee ranging from $200 to $7,000 to get Reliability Program seal
- There are currently 51,600 Web sites that are accredited as meeting the BBBOnLine standards

BBB Online Seal

TRUSTe

- Web site must agree to comply with TRUSTe's oversight and consumer resolution process
- Pay an annual fee.
- mid-2008: TRUSTe converted to for-profit status, selling approximately $10 million (to Accel Partners)
- Criticized TRUSTe because:
  - It rarely tells users when a Web site has been removed from its program
  - It doesn't require its member Web sites to give users a choice to opt out in some conditions
- There are currently 1,500 Web sites accredited by TRUSTe

TRUSTe Seal


ONESKY JETS
Latitude Membership
Flexibility. Choice. Value.
Flight Planner
Which is more important, price or schedule?
Price
Select a Trip Type
Round Trip
One Way
Empty-Leg
Multi-Leg
Origin City or Airport Code
Departure Date and Time
8:00am
Destination City or Airport Code
Return Date and Time
4:00pm
Passengers
1
Questions? Click Here for Live Chat
Continue
TRUSTe
CERTIFIED PRIVACY
MEMBERSHIP PROGRAMS
APPROVED AIRCRAFT
SAFETY
ABOUT US
NEWS & EVENTS
AIRCRAFT SALES
OneSky Jets Company Profile
OneSky Jets is uniting the country's best aircraft charter operators into a national network and giving travelers the tools they need to charter private jets with confidence and ease. OneSky's executive team has more than one hundred years of management experience in the aviation and technology industries. As passionate advocates for modernizing the air charter industry, they focused on what was missing in the marketplace:
An unparalleled choice of planes and features
A state-of-the-art reservations site
A system to provide price quotes in seconds
A supply network of Part 135 air carriers to deliver coast-to-coast service
Competitive pricing - adjusted for the demand in a given market. OneSky.com was designed as the smart choice for personal and business travel.
We Are Changing the Industry
The traditional air charter industry consists of hundreds of small, regional air carriers. We believed it was time for private-jet customers to benefit from the Internet and the growing trend towards national brands. In other industries, a national brand means that customers benefit from economies of scale that result in better pricing. But we realized that the aircraft charter industry was behind the curve, with outdated reservation systems. We also recognized that private-jet passengers were paying too much with flight card and fractional ownership programs. All of the national programs are priced significantly higher than what OneSky can deliver. OneSky Jets is dedicated to
About Us
OneSky Jets Company Profile
Membership Programs
Management Team
Career Opportunities
News
Contact Us

Access to Government Records

1. Freedom of Information Act (FOIA) (1966, amended 1974)
   - grants citizens the right to access certain information and records of the federal government upon request.
   - U.S. citizens filed 2.7 million requests for government data using FOIA procedures

2. Privacy Act of 1974
   - Prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system
   - The CIA and law enforcement agencies are excluded from this act