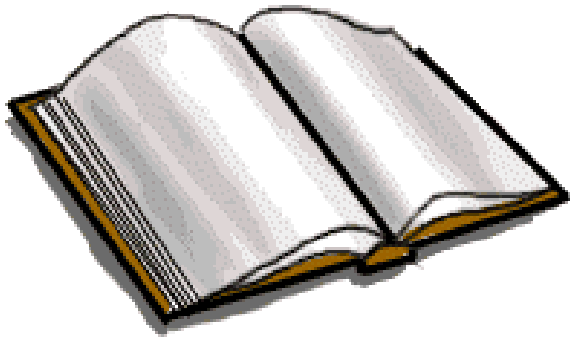
Personally Identifiable Information (PII)

Course Objectives

- Identifying Personally Identifiable Information (PII)
- Safeguarding Procedures of PII
- Reporting PII Breaches
- Proper disposal of PII

References



- Privacy Act of 1974
- DA PAM 25-51, Army Privacy Program
- DoD 5400.11-R, DoD Privacy Act Program, May 07
- DoD Policy Memo, Safeguarding Against and Responding to the Breach of PII
- AR 340-21, Army Privacy Program
- OMB, M-07-16, Safeguarding Against and Responding to the Breach of PII, 22 May 2007
- DA, Alaract 050/2009, PII Incident Reporting and Notification Procedures
- https://www.rmda.army.mil/programs/privacy.shtml Army Privacy Program
- http://iase.disa.mil/eta/piiv2/launchpage.htm Identifying and Safeguarding PII Version 2.0 interactive presentation

Overview of the Privacy Act of 1974

Privacy Act of 1974 *safeguards individual privacy* contained in Federal records and *provides* individuals *access* and amendment *rights to records* concerning them which are maintained by Federal agencies.

Privacy Act Statement

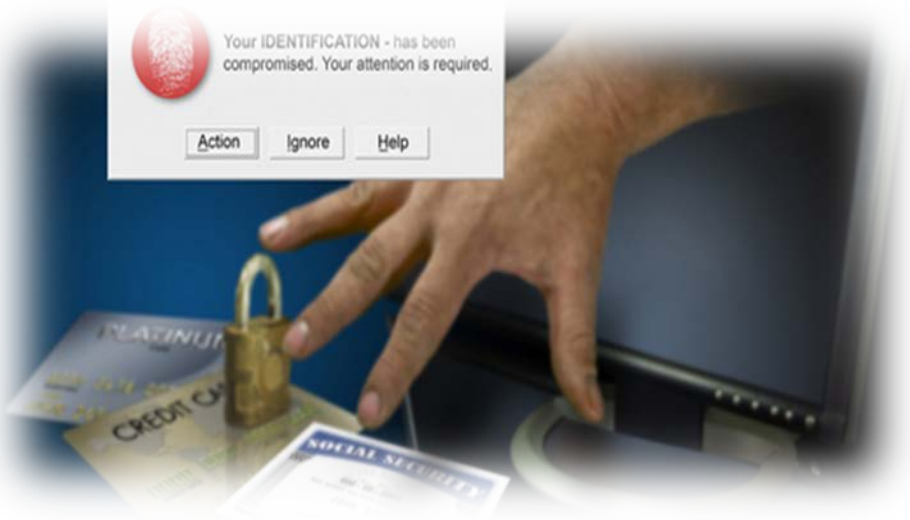
The Privacy Act requires that when an agency solicits information from an individual for a system of records the individual must be provided:

1. The statute or executive order of the President;
2. Principal purposes for which the information is intended to be used;
3. Routine uses which may be made of the information as published in the System of Records Notice (SORN) in the Federal Register;
4. Whether the disclosure of the information is mandatory or voluntary; and the effects if any, on the individual for not providing the information.

Overview of the Privacy Act of 1974

Routine Use - Release of information outside the agency for a purpose compatible with the purpose for which the information was collected

The Privacy Act *prohibits* disclosing personal information to anyone other than the subject of the record without his or her *written consent*

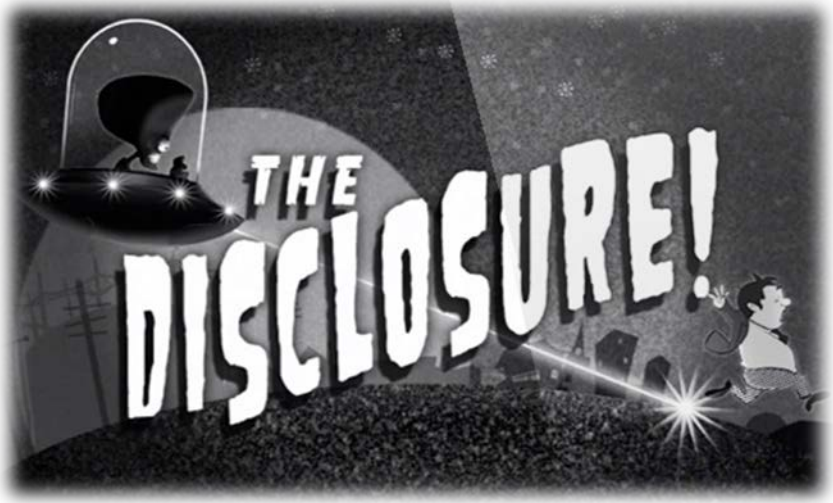


There are twelve exceptions to the "*no disclosure without consent*" rule. Those exceptions permit release of personal information *without* the individual's consent

Overview of the Privacy Act of 1974

Disclosure

✓ No agency shall *disclose any record* which is contained in a system of records by any means of communication to any person or another agency *without* a written request or prior written consent of the individual to whom the record pertains unless the release has been established by a routine use.



✓Disclosure includes *any means* of communication -- oral, written, or electronic.

✓ Disclosure *does not* occur if the communication is to those who already know.

What Is PII?

PII

SSN: 999-99-9999

Biometrics

Personally Identifiable Information (PII):

information that can be used to distinguish or trace an individual's identity

How is PII stored?

- Records
- System of records

Who uses PII?

- Only individuals with a need-to-know

Definition for Personally Identifiable Information (PII)?

Answer

PII is information about an *individual* that *identifies, links, relates, or is unique to, or describes him or her*.

PII can be *hard copy* or *electronic* records stored within databases or other applications on computers, laptops, and personal electronic devices such as blackberries.

Examples of PII

Personally Identifiable Information is *any information* about an individual maintained by an agency, some ***sensitive*** PII include, but not limited to the following:

- ✓ Name and other names used
- ✓ Social security number, full and truncated
- ✓ Citizenship, legal status, gender, race/ethnicity
- ✓ Birth date, place of birth
- ✓ Home and personal cell telephone numbers
- ✓ Personal email address; mailing and home address
- ✓ Religious preference; Security clearance
- ✓ Biometric records, including spouse information, marital status, child information, emergency contact information

- ✓ Education
- ✓ Mother's middle and maiden names
- ✓ Financial, medical, or disability information
- ✓ Criminal or employment history and information which can be used to distinguish or trace an individual's identity.
- ✓ Military records

Examples of Releasable PII

Examples included, but *not limited* to:

- ✓ Office location
- ✓ Business telephone numbers
- ✓ Business email address (generic)
- ✓ Badge number (official capacity)

Can You Breach Your Own PII?

Answer - No, you can not!!

What are the consequences of stolen, loss or compromised PII?

Collecting PII

If you collect it, you must protect it!!

If in doubt, leave it out!!

Do You Know Your Responsibilities for Protecting Personal Information?

Storing PII

Duty Hours

- ✓ Cover with *DD Form 2923* (Privacy Act Cover Sheet) or *DA Label 87 (FOR OFFICIAL USE ONLY)* or place in an out-of-sight location when those not authorized access enter the work space.
- ✓ Use privacy shield devices on computer screens to limit visibility.
- ✓ Lock computers when leaving – even for brief periods.
- ✓ When emailing PII, emails must be *encrypted.*

After Duty Hours

- ✓ Records (i.e. hard copy, CDs and DVDs) should be placed in a locked drawer, cabinet or office.

Special Categories of PII Personnel Files

- ✓ Investigative Files
- ✓ Security Clearance Files
- ✓ Adverse Action Files
- ✓ Medical Records
- ✓ Any collection of PII that may confer or deny benefits to an individual.

Sharing PII

Follow the ***"Need-to-Know"*** principle. Share only with those specific DoD employees who need the data to perform official, assigned duties.

If you have *doubts* about sharing data, consult with your supervisor or your component Privacy Officer

E-MAILS CONTAINING PII/PA/FOIA

- IT IS YOUR RESPONSIBILITY TO APPLY THE NOTIFICATION BELOW ON ALL E-MAILS CONTAINING INFORMATION SUBJECT TO THE PRIVACY ACT, FREEDOM OF INFORMATION ACT OR CONTAINING PERSONALLY IDENTIFYING INFORMATION:

- **ATTENTION:** The information contained in this communication and any accompanying attachments is intended for the sole use of the named addresses/recipients to whom it is addressed in their conduct of official business of the United States Government. This communication may contain information that is exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552 and the Privacy Act, 5 U.S.C.552a. Addressees/recipients are not to disseminate this communication to individuals other than those who have an official need to know the information in the course of their official government duties. If you received this communication in error, any disclosure, copying, distribution, or the taking of any action on this information is prohibited. If you received this confidential electronic mailing in error, please notify the sender by a “reply to sender only” message, delete this email immediately and destroy all electronic and hard copies of the communication, including attachments.

E-MAILS NOT CONTAINING PRIVACY ACT, FOIA OR PII INFORMATION

- IT IS YOUR RESPONSIBILITY TO APPLY THE NOTIFICATION BELOW ON ALL E-MAILS **NOT** CONTAINING INFORMATION SUBJECT TO THE PRIVACY ACT, FREEDOM OF INFORMATION ACT OR CONTAINING PERSONALLY IDENTIFYING INFORMATION:

- **ATTENTION:** This E-mail message, including any attachments, is for the sole use of the intended recipient (s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Transporting PII

Using E-mail: Use Common Access Card procedures

- ✓ Announce in the opening line of the text that FOUO information is contained and **encrypt** the e-mail before sending

Hand Carrying

- ✓ Use *DD Form 2923*, Privacy Act Data Cover Sheet, to shield contents

Using Ground Mail:

- ✓ Use Kraft or white envelopes
- ✓ May be double wrapped if deemed appropriate
- ✓ Mark the envelope to the attention of the authorized recipient
- ✓ Never use “holey joes” or messenger-type envelopes
- ✓ Never indicate on the outer envelope that it contains PII

Disposing of PII

Disposing of PII you can use any means that *prevents inadvertent compromise*. A disposal method is considered adequate if it renders the information ***unrecognizable or beyond reconstruction***.

Disposal methods may include:

- ✓ Burning
- ✓ Melting
- ✓ Chemical decomposition
- ✓ Pulping
- ✓ Pulverizing
- ✓ Shredding (GSA approved shredder)
- ✓ Mutilation
- ✓ Delete/Empty Recycle Bin

Disposing of PII

DO NOT Throw Out (Sensitive PII that may cause harm to an individual if lost/compromised):

- ✓ Financial information: bank account credit card, and/or bank routing number
- ✓ Medical data: diagnoses, treatment, medical history
- ✓ SSN (full or last four digits)
- ✓ Personnel ratings and pay pool information
- ✓ Place and date of birth
- ✓ Mother's maiden name
- ✓ Passport number
- ✓ Security clearance info

Examples of what ***NOT*** to throw out are:

- Voided or returned checks
- Defense travel forms
- Personal resumes
- Recall rosters and etc.

Personally Identifiable Information

If ***You*** Have Access to Personally Identifiable Information

If you Collect it, you must Protect it!!

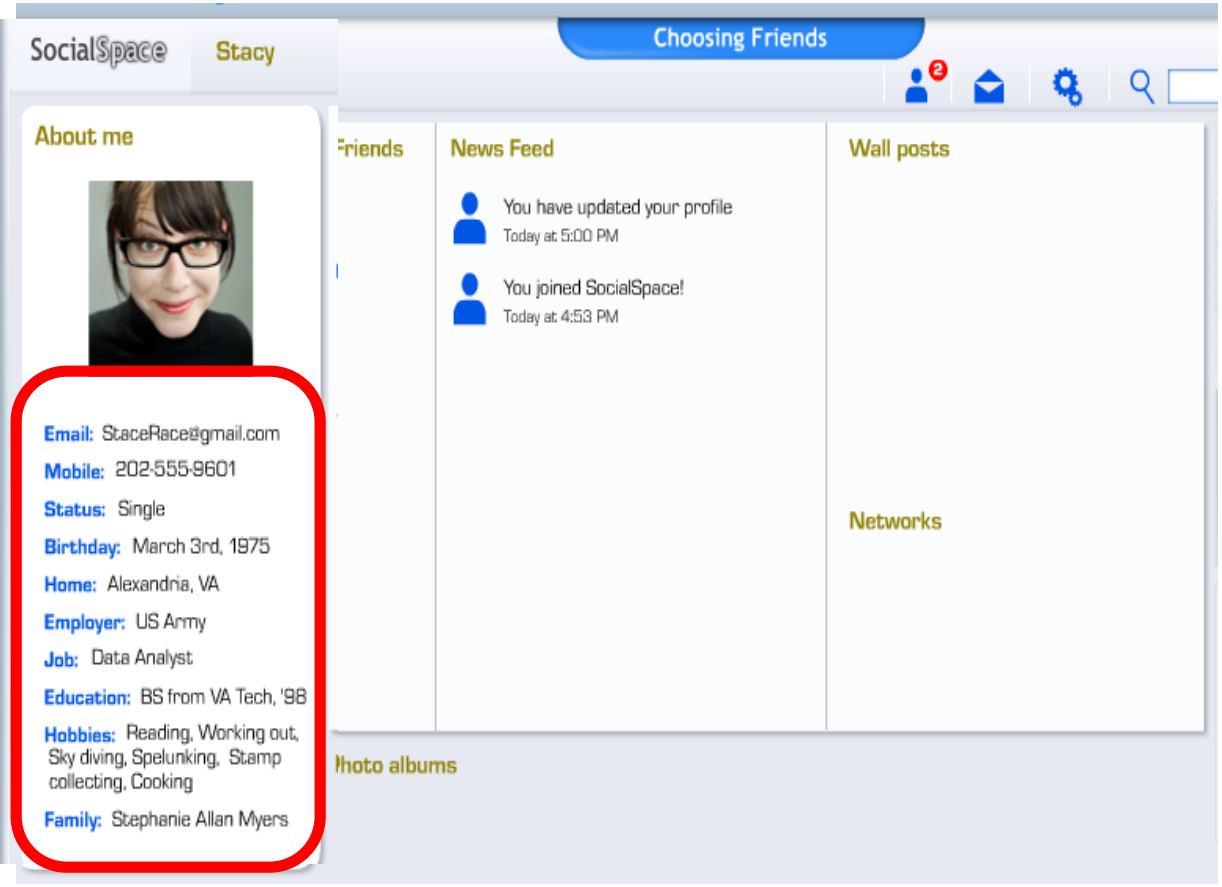
If in doubt, leave it out!!

Social Networking Services

Social Networking Services

- These are programs that allow people to connect through the internet or mobile devices (i.e. Twitter, Face book)
- Free, easy to use and became a big part of our daily lives
- Engrained in our nations institutions (i.e. elected officials to Federal agency personnel)
- People fill out in-depth profiles
- There are risks

Social Networking Lessons Learned



- ✓ Always consider how information on your *profile* can affect your personal security or OPSEC.
- ✓ Remember you are personally responsible for what you post and information can be exposed or stolen.
- ✓ *Profiles* pose a huge identity theft risk.
- ✓ Limit posting personal information (PII).

By providing too much PII someone can impersonate YOU or guess your password!

Privacy Breach

Definition

Breach – possible or actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII or covered information, whether physical or electronic.

Main Cause of PII Breach

Human error is the cause of 80 percent of the PII breaches. Not knowing or not following ***guidance***, or just being ***careless*** can result in the unintended disclosure of privacy sensitive information and potentially adversely affect many personnel.

The ***Social Security number*** is the ***most*** frequently lost, stolen or compromised PII data element.
The SSN is involved in almost 70 percent of breaches.
This sensitive identifier *must be closely safeguarded* or *eliminated* from use.

SSNs are improperly disclosed by: sending SSNs in an email or in attachments, creating recall rosters with SSNs, or posting names with associated SSNs to web portals or shared drives. In these examples, SSNs were either *transmitted without encryption*, *not properly marked* or sent to recipients that did not have a *need to know*.

Examples of Internal Breaches

- ✓ 5 Laptops used for testing were stolen from off-post testing facility. The laptops contained PII (name, SSN, DOB, address, email, and phone number) of 120 Soldiers
- ✓ Payroll information distributed improperly.
- ✓ E-mail messages containing attachments with PII went to a group of persons *without authorization* or a *"need to know"*
- ✓ Military photos posted Facebook.

Your Goal/Our Goal: 0 Breaches!

Reported External PII Breaches

FederalComputerWeek

FAA suffers massive data breach; more than 45,000 affected

Feb 10, 2009

The Federal Aviation Administration has notified employees that one of its computers was hacked, and the personally identifiable information of more than 45,000 employees and retirees was stolen electronically.

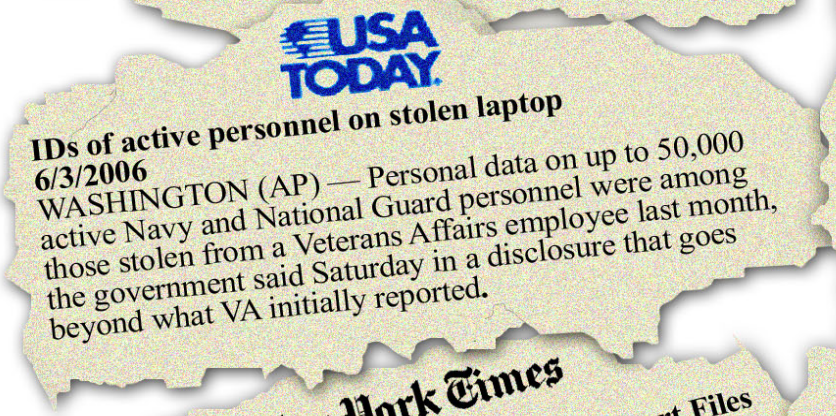
BBC WORLD

BBC News

Job website hit by major breach?

August 21, 2007

US job website Monster.com has suffered an online attack with the personal data of hundreds of thousands of users stolen

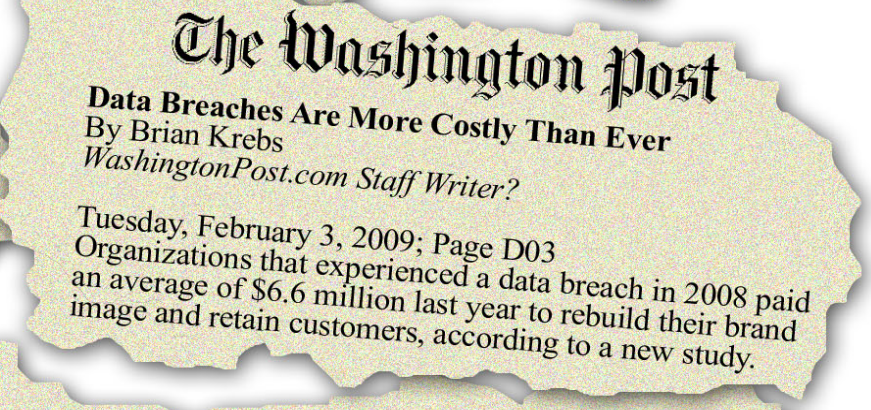


USA TODAY

IDs of active personnel on stolen laptop

6/3/2006

WASHINGTON (AP) — Personal data on up to 50,000 active Navy and National Guard personnel were among those stolen from a Veterans Affairs employee last month, the government said Saturday in a disclosure that goes beyond what VA initially reported.



The Washington Post

Data Breaches Are More Costly Than Ever

By Brian Krebs

WashingtonPost.com Staff Writer?

Tuesday, February 3, 2009; Page D03

Organizations that experienced a data breach in 2008 paid an average of $6.6 million last year to rebuild their brand image and retain customers, according to a new study.

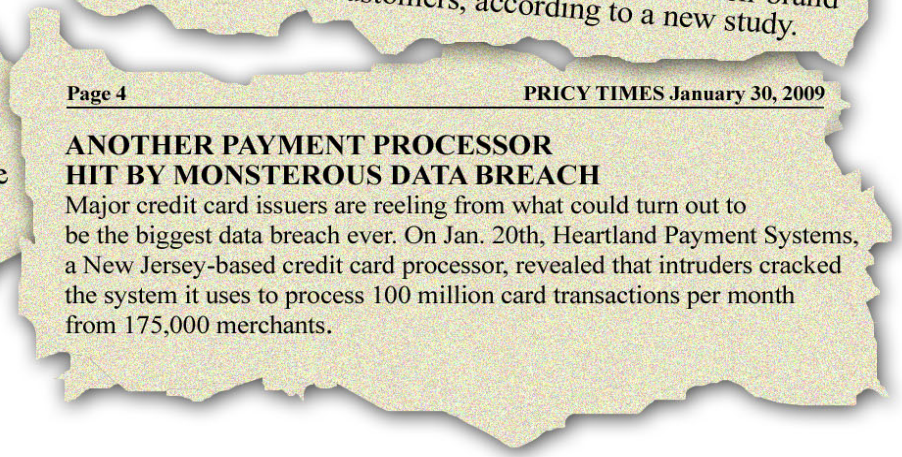
The New York Times

September 23, 2008

Ex-Employee Pleads Guilty to Viewing Passport Files

By ERIC LICHTBLAU

A former foreign service officer at the State Department pleaded guilty on Monday to illegally reading the private passport files of three presidential candidates as well as those of actors, athletes and media figures.



Page 4 **PRICY TIMES January 30, 2009**

ANOTHER PAYMENT PROCESSOR HIT BY MONSTEROUS DATA BREACH

Major credit card issuers are reeling from what could turn out to be the biggest data breach ever. On Jan. 20th, Heartland Payment Systems, a New Jersey-based credit card processor, revealed that intruders cracked the system it uses to process 100 million card transactions per month from 175,000 merchants.

Procedures for a Suspected Breach

A PII breach must be reported immediately!

✓ Within ***one hour*** of discovery report incidents whether suspected or confirmed to United States Computer Emergency Readiness Team (US-CERT) and simultaneously , an email will be sent to the Records Management and declassification Agency (RMDA) which notifies Army leadership that an initial report has been submitted.

✓ Follow internal command procedures. IMCOM Reg 190-1 at https://www.us.army.mil/suite/doc/12451407

Procedures for a Suspected Breach

Within one ***hour*** of discovery report incidents whether suspected or confirmed contact your Privacy Act Officer and immediate supervisor:

PII Breach Steps Must Be Completed Within One Hour!

Step 1: Go to http://www.us-cert.gov/
Step 2: Click “Government”
Step 3: Click on “Report an Incident” –for all breaches
- Skip those areas that require specific information
- Your synopsis should answer the five Ws.

Step 4: Once you complete the form you will receive a US-CERT number like this (**2013-USCERTv33HYWVP)** save this number; you are going to need it later.
Step 5: Print out copy of form sent to US Cert
Step 6: You will then report to the DA Privacy Office the reported breach. Go to https://www.rmda.army.mil/privacy/RMDA-PO-Division.html. Click report a PII Breach.
Step 7: Please send the USCERT and DA PA report to the Installation PII Officer so that the office can track this breach.

Note: If during the initial investigation PII has been released, the command makes the final decision that notifying affected personnel is warranted, a sample notification letter can be obtained at the following link: https://www.rmda.army.mil/organization/pa-guidance.shtml

Point of Contact

- Maureen Barefield, FOIA/PA Officer
- Phone: 706-545-5356
- Email: maureen.a.barefield2.civ@mail.mil

CERTIFICATE OF INITIAL/ANNUAL REFRESHER TRAINING

- This is to certify that I have received initial/annual refresher training on my privacy and security responsibilities. I understand that I am responsible for safeguarding personally identifiable information that I may have access to while performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard personally identifiable information, for improperly using or disclosing such information, and for failure to report any known or suspected loss or the unauthorized disclosure of such information.

- _____ _____
- (Signature) (Print Name)

- _____ _____
- (Date) (DoD Component/Office)