



Surveillance and Falsification Implications for Open Source Intelligence Investigation

F15011007 Fatih Adıyaman
11011028 Mustafa Safa Fındık
13011605 Gizem Sivari
100110059 Gökçe Karakaya

WHAT IS THE OSINT?



- Open Source Intelligence is very important to use many sources for information.
- Processing and Filtering=Information
- All information is not quality of OSINT
- Actually OSINT is very important for our life

- **So WHY is OSINT important?**

- Cheap

- Easy to gather information

- Not necessary to hide informations

- Constitute 90% of the informations

- **Types of Informations**

- Open Source**

- *Media Source

- Newspaper, Radio, TV

- *Social Tools

- Blogs, Sites, Sharing Data

- *Public Data

- Government reports, Formal Data

- Covered Source**

- **If any information supply at least one of these rules;**
 - As a counter for obtaining should not be
 - Must be free or very little compensation
 - Must be easily obtained by anyone
 - Protection or storage should not be concerned
 - Not have the confidential degree

It is an OSINT.

- **OSINT consists of four basic elements;**
 - Uncovering**
 - *Where we can find the information
 - Discrimination**
 - *Separation of resources
 - Refining**
 - *Information should be as short as a paragraph
 - Delivery**
 - *To send the information to customer

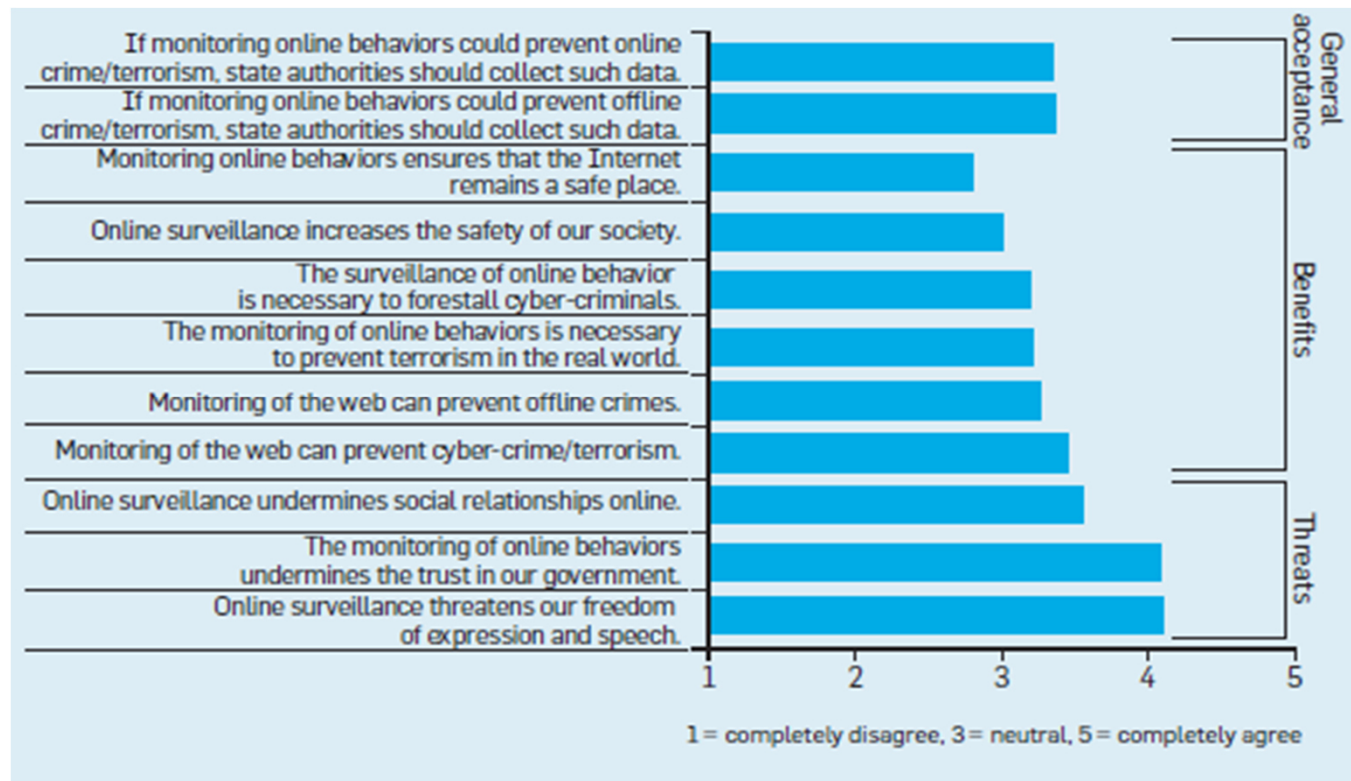
- **Where can we use the OSINT?**
 - Business Intelligence**
 - *Opponent Analysis
 - *Potential Customer Analysis
 - Government Intelligence**
 - *Military and Political information
 - Individual Intelligence**
 - * Personal information



STUDY DESIGN AND SAMPLE

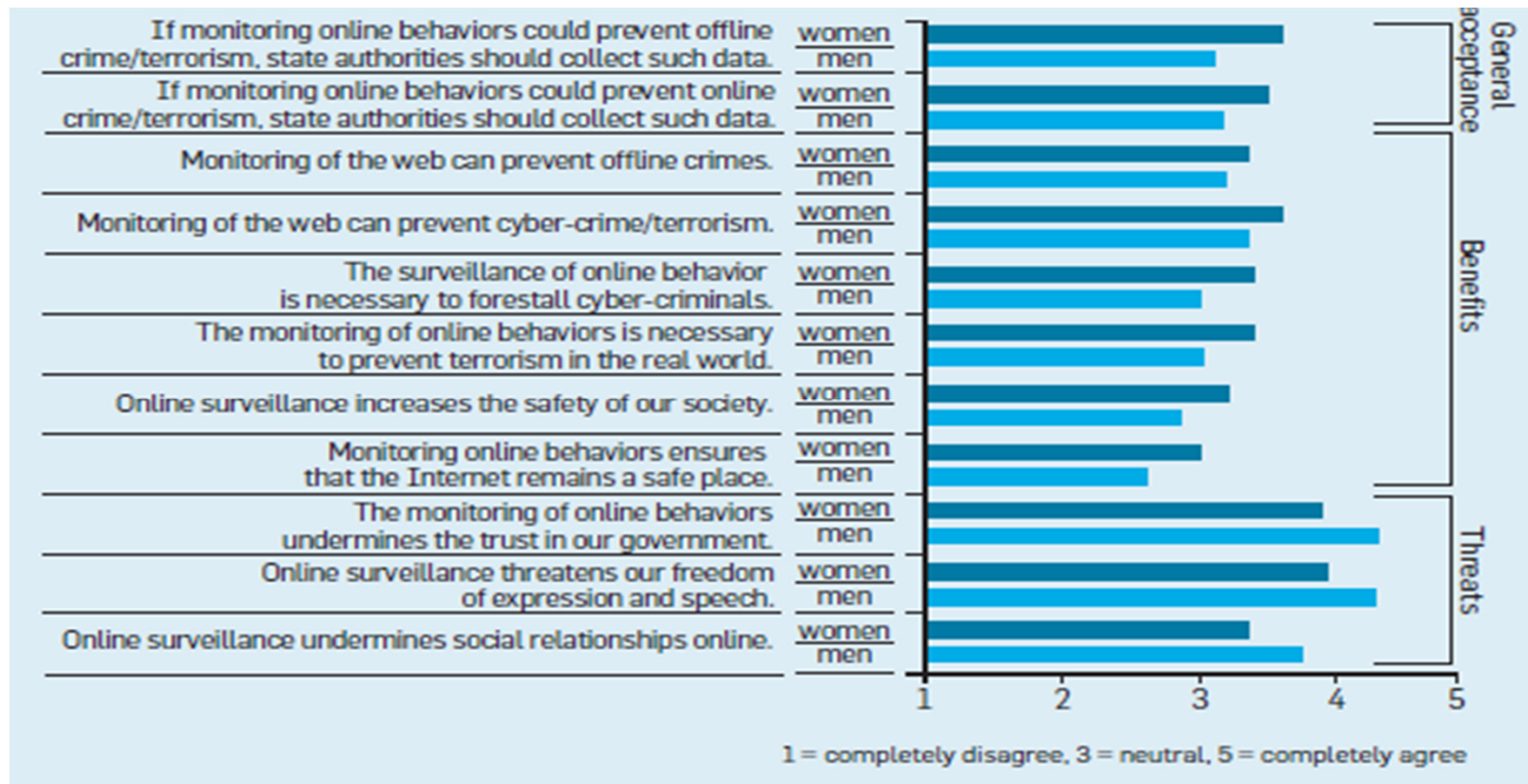
- To understand the Internet users' attitudes toward personal information in connection with online surveillance,



When you think about the possibility of state authorities monitoring your online behaviors, how much do you agree with these statements?



For  ??? For  ???



Attitudes toward online surveillance by state agencies

Surveillance by *state agencies vs. private companies*





Degree of acceptance and
propensity to falsify personal
information online





**FALSE
NAME**

**FAKE E-
MAIL
ADDRESS**

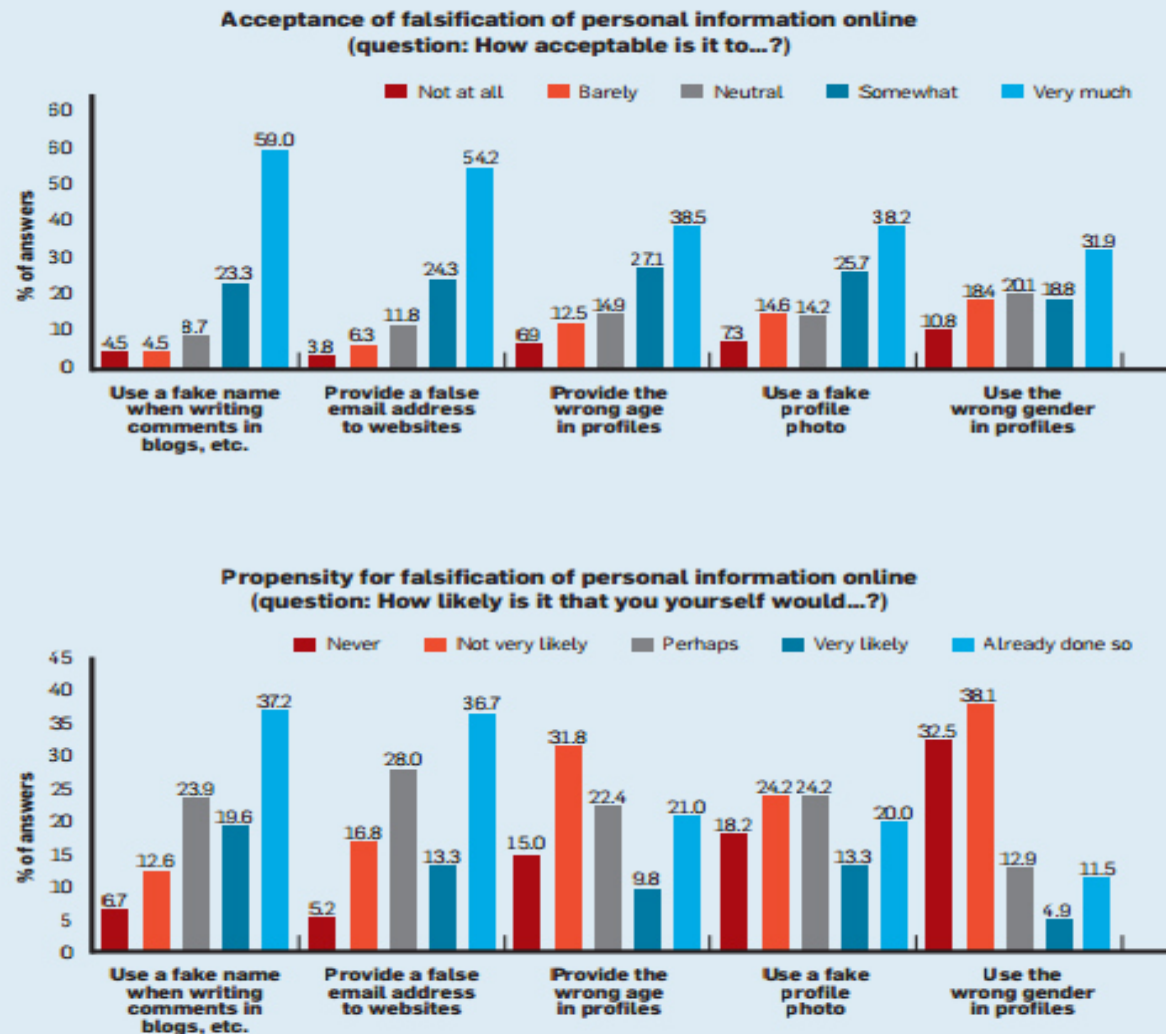
**WRONG
AGE**

**FAKE
PHOTO**

**WRONG
GENDER**

- **How acceptable is it to falsify personal online information?**
- **How likely are you to falsify your own personal information online?**

Figure 4. Acceptance and propensity for falsification of personal information among all participants.



The questions on degree of surveillance awareness and falsification acceptance and propensity referred to different entities;



NO MENTION
OF AN
ORGANIZATION



SURVEILLANCE
BY PRIVATE
COMPANIES



SURVEILLANCE
BY STATE
AGENCIES



Linking information falsification with surveillance assumptions and attitudes



Correlations between falsification behaviors and online surveillance assumptions and attitudes.

Generic condition (no mention of an organization; n = 91)

	Mean	Std. dev.	1.	2.
1. Assumption of online surveillance	3.36	0.88		
2. Acceptance of information falsification	3.80	1.06	.22	
3. Propensity for information falsification	3.02	1.03	.10	.66**

Condition "surveillance by private companies" (n = 103)

	Mean	Std. dev.	1.	2.
1. Assumption of online surveillance	3.52	0.73		
2. Acceptance of information falsification	3.99	0.96	.13	
3. Propensity for information falsification	3.26	1.03	.12	.63**

Condition "surveillance by state agencies" (n = 104)

	Mean	Std. dev.	1.	2.	3.	4.	5.
1. Assumption of online surveillance	3.13	0.96					
2. General acceptance of online surveillance by state agencies	3.23	1.22	-.04				
3. Benefits from surveillance	3.06	1.02	.01	.78**			
4. Threats from surveillance	4.05	0.79	.11	-.38**	-.49**		
5. Acceptance of information falsification	3.84	0.96	.08	-.32**	-.24**	.21*	
6. Propensity for information falsification	2.92	1.07	.24*	-.26**	-.23*	.13	.59**

* p < .05

** p < .01; Pearson correlations, two-sided tests

- While surveillance awareness alone may lead to information falsification, the main trigger to falsifying personal information seems to be the extent surveillance is seen as (in)appropriate.

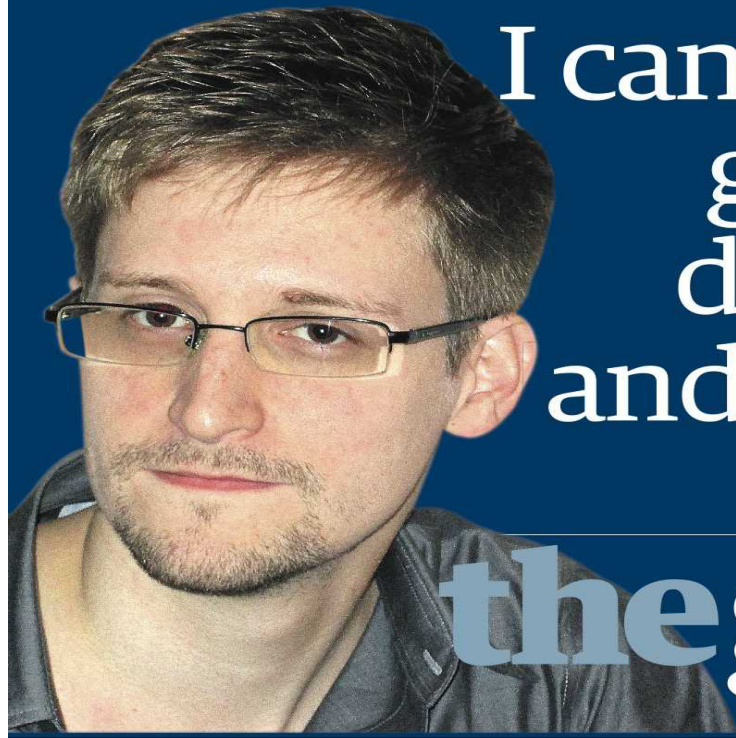


MORE THAN A MORAL DILEMMA



PRIVACY vs. RIGHTFULNESS

The whistleblower



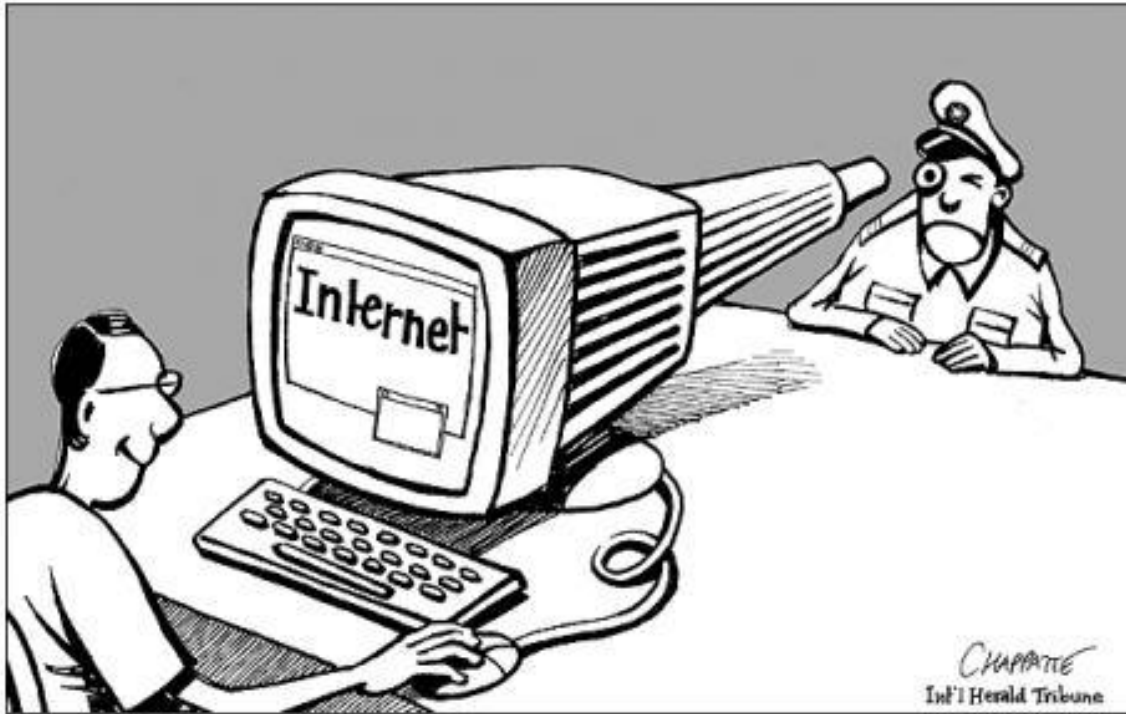
I can't allow the US
government to
destroy privacy
and basic liberties

the guardian

guardian.co.uk

"America is that nothing will change."

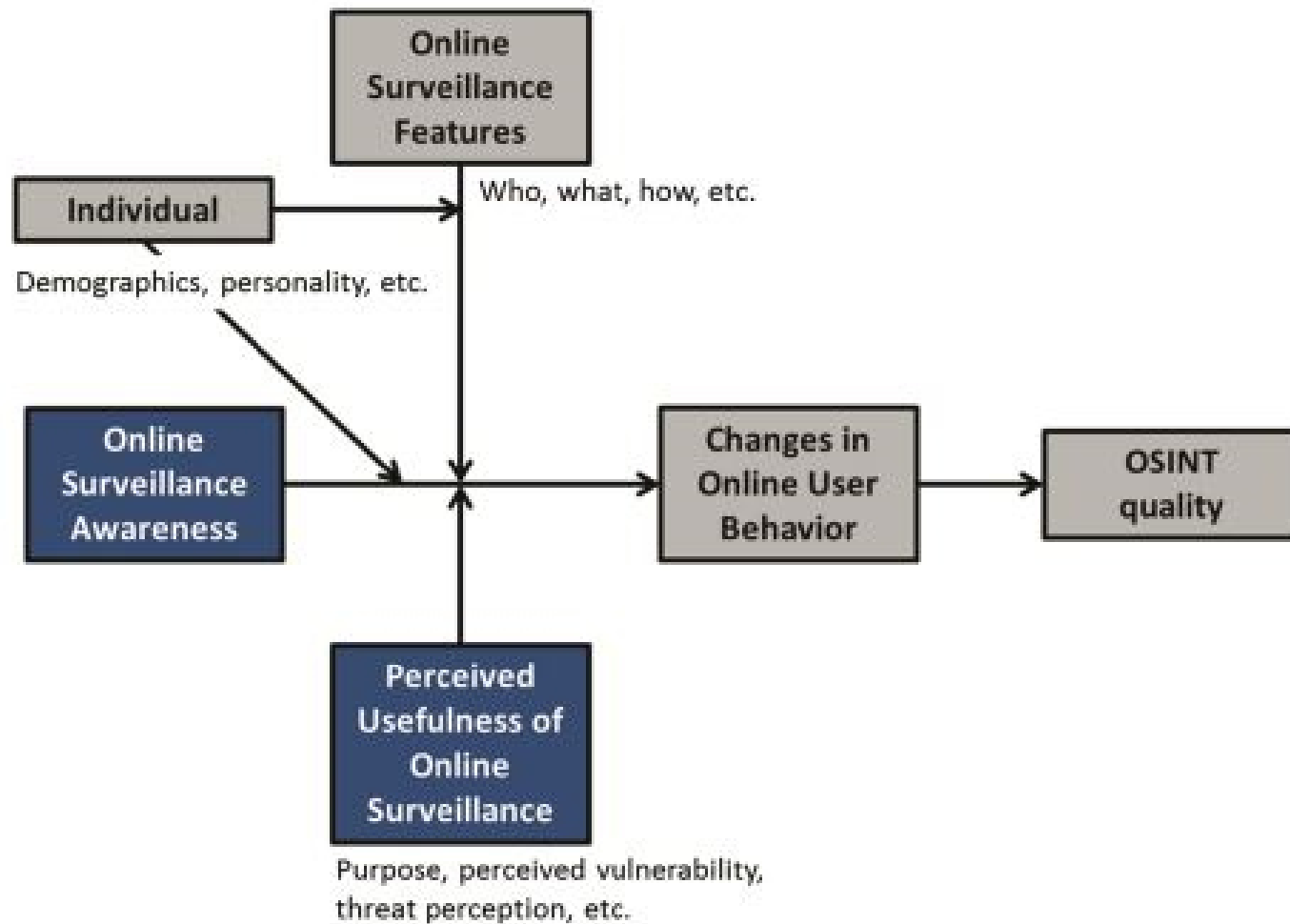
- Validity of online data?
- Is surveillance neutral?



OSINT is «no cost» but;

- Awareness of Online Surveillance reduce OSINT's benefits





TECHNICAL SOLUTIONS

- Trust Score Computation
- Validity Pattern Mining
- Classification Mining
- Association Rule Learning



- Where did the data come from?
- How trustworthy is the original data source?
- Who handled the data?
- Are the data managers trustworthy?



How to identify false information with technical methods?



- Possible links between profiles. Twitter-Facebook etc.
- Same Pseudonym
- Social graph

AN INTERESTING QUESTION

- How «Volatile» is Fallsification?



Technical Solutions are Complex and Costly.



IN BRIEF

- OSINT is still valuable for investigation processes
- Advanced Technical solutions is not the «Solution»

WHAT SHOULD BE DONE

- Make clear what is the perceived purpose and legitimacy of surveillance
- Reduce distrust in law-enforcement agencies



**KEEP
CALM
AND
LEARN TO LOVE
THE NSA**