-뉴미디어 연구회 스터디 발제(2016.09.10) 김은영

<당신은 데이터의 주인이 아니다>
- 2 부: 지금 무엇이 위험한가.

* 도처에서 이루어지는 대량감시로 인해 발생하는 피해를 다룸.

7 장...정부의 감시로 인한 피해

1) 국민에 대한 무제한의 대량감시를 정부에 허용할 때 발생하는 위험 제시
2) NSA 의 감시 = 자기면역성 질환(Yochai Benkler) → 자유가 가장 큰 희생
3) 데이터에 의한 고소
 - 일반영장/투망식 수사와 유사: 대량의 데이터 생성과 무기한 저장으로 모든 이력의 영원한 기록, 불리한 증거로 권력자들의 학대 가능성.
 - '특징 공격(signature strike)': 식별가능한 나이, 성별, 현재의 행동이나 개인별 특징을 근거로 신원 미상의 사람들을 표적 → 무기한 감시의 대상화.
4) 정부의 검열:
 - 자유와 생각의 자유로운 전달 억압. e.g) 중국 '만리방화벽(Great Firewall of China)'
 - 과도한 자기검열
5) 냉각효과
 - 언론 및 사상의 자유를 침해.
 - 감시는 협박의 전술: 뉴스 보도 위축, 민감한 용어 검색의 가능성 축소(개인).
 - 표현의 자유와 결사의 자유를 포함한 인권에 냉각효과
 - 파놉티콘: 개성을 잃고 사회는 퇴보, 순종적/복종적, 자유를 누리지 못함.
6) 반대자도 발전도 없는 사회
 - 정치적 담론 훼손.
 - "결점이야말로 자유의 핵심적인 차원": eg. 동성결혼과 마리화나 이용.
7) 모든 것이 기밀이 되다
 - 정부의 기밀주의 발현 방식: 기밀의 범위 확대와 폭발적 증가, 기밀의 과도한 적용, 정부가 기밀 폭로한 내부고발자에 대한 가혹한 처사
8) 감시 능력의 남용
 - 감시 시스템의 남용, 감시 조직안에서의 남용.
 - 거대하고 강력한 관료 체제가 확장되면서 권력도 함께 확대: "계획하지 않은 임무 변경(mission creep) "병행구성(parallel construction)"
9) 인터넷자유가 위협받고 있다
 - 억압적 국가들이 미국의 감시를 근거로 자신의 가혹한 인터넷 정책을 정당화. → 고립주의적 인터넷 정책
 -인터넷 자유는 인권 문제이며 미국 지지 필요.
→ 인터넷은 세계적으로 소극적/적극적 자유의 동인이자, 감시로 잠재력이 낭비됨.

8 장...규제받지 않는 기업의 감시로 인한 피해

1) 감시에 기반한 차별
 (1) 기업은 감시 데이터를 이용하여 차별
 - 범주화에 따른 상품과 서비스 차별화. 레드라이닝(redlining) → 웹라이닝(weblining).
 - 사회 관계에 따른 평가.
 - "감시 분류 기술(panoptic sort)" : 차별적 기준을 이용하여 서로 다른 기회와 접근권, 자격, 가격, 관심, 그리고 노출도를 분배하는 힘(Oscar Gandy, 1993).
 - 고용주와 직원 관계에서 침해 증가: 사업장의 노동 감시

(2) 고객들은 판매자들이 고객의 주머니를 열기 위해 서로 경쟁하고, 소프트웨어 시스템이 가격 차별을 더욱 용이하게 하며, 고객에게 차별을 숨기는 한 기업의 감시에 따른 차별 지속

2) 우리의 심리를 조종하는 인터넷 기업

- 감시는 통제를 용이하게 함
- 소셜네트워킹 플랫폼의 조작 가능성: 대중의 담론 왜곡 가능. e.g) 중국 '우마오당', 삼성.
- "필터 버블(filter bubble) 현상: 인터넷이 사용자의 선호도에 맞게 최적화되어 자신이 동의하지 않는 견해는 결코 접할 필요가 없어지는 현상. → 중앙 집중적인 의사소통 구조로 통제 용이.
- 프라이버시의 침해: 정보가 보호되는가? 국제적 사이버범죄(신용 도용, 해커) 등.

➔ 기업들이 인터넷의 여러 '장소'를 통제하고, 데이터를 기업의 이익을 위해 이용하고, 기업은 우리를 분류하라고 조종. 조종은 규제없이 모르게, 기술 발달로 효율화 됨

9 장… 기업 경쟁력

1) 클리퍼 칩과 암호키 위탁 시스템의 실패는 강력한 암호 기법에 대한 미국 정부의 규제의 종료 → 외국 경쟁업체라는 위협과 미국 업계의 요구로 폐지.

2) 정부의 감시가 기업에 끼치는 손해 : 사람들이 미국 클라우드 제공업체들을 회피, 미국의 컴퓨터와 네트워킹 장비 구매 거부, 미국 업체를 불신 → 데이터 프라이버시는 국제 상거래의 새로운 공적 안전요건이 될 것임.

3) 기업의 감시가 사업에 끼는 손해: 시장 차별화 요소로 프라이버시 보호를 제시하는 기업의 등장. 정보보호 최고책임자 고용

➔ 미국의 감시에서 스스로를 지키는 과정에서 미국 기업의 경제적 피해가 발생함. 자국의 데이터 보호를 위해 국가 장벽을 세우는 독일/브라일의 사례는 미국 기업에 큰 손해를 끼침.

10 장… 프라이버시 상실이 초래하는 피해

1) "숨길게 없는 사람은 두려워할 것도 없다"(감시 지지자- 동독 비밀경찰 슈타지, 칠레의 독재자 피노체트, 구글 에릭 슈미트).

2) 프라이버시는 인간 본연의 권리, 존엄과 존중 속에 인간의 조건을 유지하는 데 필수적. 프라이시 성취가 곧 힘의 표현.

3) 프라이버시의 침해는 맥락이 중요. 동일하게 해로운 것은 아님.

4) 영원히 사라지지 않는 대화

- 통제할 수 없는 방식으로 대화가 저장.
- 선사 시대의 종말(Charles Stross): 우리의 모든 말과 행동이 우리와 영원히 연관될 것을 의미. → 망각이 없는, 사회적, 심리적인 변화를 겪을 것임.

5) 사람이 아닌 컴퓨터가 감시하면 괜찮을까? NO!

- 컴퓨터는 자기가 보는 것을 처리하고 있으며 그것을 기초로 행동을 함. 데이터를 저장하지 않음을, 인지하는 사람이 없다는 점을, 컴퓨터가 본 것을 기초로 평가 혹은 차별을 받지 않는다는 확신할 수 없음.
- 컴퓨터의 데이터 보관은 폭로될 위험 상존.
- 실제로 누군가가 우리의 데이터를 보는지 여부와 상관없이 알고리즘 배후에 있는 사람이 그렇게 할 수 있고, 그들이 알고리즘을 이끌어간다는 바로 그 사실 때문에 이 상황은 감시에 해당

6) 인터넷 실명화라는 불가능한 목표

- 사람들이 신원을 확인받고 싶어함
- 인터넷의 데이터 패킷마다 식별용 정보 부착의 어려움, 지구상 어딘가의 사람의 신원 확인의 어려움 등은 인터넷의 작동 방식 자체에 내재된 문제.

(3) 신원확인 인프라스트럭처가 없음.
➔ 양가적인 익명성: 편파적 발언과 범죄 활동을 보호/ 프라이버시 보호와 개인에게 힘을 주며, 자유의 필수적인 요소

11 장… 감시로 인한 보안 측면에서의 피해

1) 드문 극적인 위협에 집중하는 경향.
2) 대량감시는 테러를 막아줄까: 데이터 마이닝의 부적합
- 오차율: 양성 오류가 시스템을 완전히 압도.수백만의 무고한 사람들이 잘못 고발됨.
- 각각의 공격이 다 특이하는 점. 기준을 흔들고, 탐지 전략의 효과 저하
- NSA 가 찾아내려는 사람들이 약삭빠르고 적발되지 않으려는 노력을 함.
3) 인터넷 공격 대 방어: 인터넷과 일반 컴퓨터에서는 공격자가 유리
- 고치기보다 부수는게 더 쉬움.
- 복잡함은 보안의 최악의 적.
- 방어자가 모든 취약점을 찾아 고치기는 어렵지만 공격자가 하나의 이용가능한 취약점을 찾기는 쉬움.
- 공격자는 특정한 공격을 선택 집중하는 반면, 방어자는 모든 가능성에 대비한 방어를 해야 함.
- 소프트웨어 보안은 대체로 형편없음.
- 컴퓨터 보안은 매우 기술적인 문제로 일반 사용자의 잘못된 이해로 기존의 보안 체계를 무력화할 수 있음.
4)보안은 결국 기본적인 경제 문제로 귀결: 비용대 편익의 관점에서 생각. 무작위 공격은 빈집털이와 유사하여 상대적인 보안, 표적 공격은 절대적인 보안 수준이 중요
5) 암호화의 가치
- 암호화 작업은 수리적 우위(암호키의 길이)에 기초. e.g) 64 비트 암호키 해독 1 일, 65 비트의 암호키 해독은 2 일, 128 비트는 2 의 64 승, 1000 조년 걸림).
- 암호화 보급은 대량감시의 효력의 감소, 도청자들은 특정 표적을 선택해야 하는 프라이버시의 승리를 가져옴.
5) 확산된 취약점
- 취약점은 설계나 실행 과정에서의 오류, 즉 코드나 하드웨어상의 결합으로, 불법적인 시스템 침투를 가능하게 함. 해킹에 이용.
- 취약점을 발견하면 방어나 공격에 이용 가능. 보완 패치 제작.
- 제로데이(zero-day)는 공식적으로 발표되지 않은 취약점을 의미. 보호와 처벌이 없어 공격자들에게 매우 소중. 해킹 위협은 상존.
6) 인터넷 보안을 훼손하는 정부: NSA 의 보안과 프라이버시 무력화 방법
- 보안상의 결합을 확실하게 고치는 대신 사람들이 일상적으로 이용하는 상용 소프트웨어의 취약점 비축(제로데이 비축, 노버스 *NOBUS*)
- 널리 사용되는 컴퓨터 하드웨어와 소프트웨어 제품에 백도어 삽입하기
- 암호화 알고리즘과 암호와 표준 약화시키기. e.g) GSM 방식전화의 암호화 알고리즘
- 인터넷 해킹하기.
- NSA 는 보안보다 감시를 우선시하여 모두를 위험 빠뜨림.
7) 콜래트럴 데미지. 국가간의 해킹은 대중(민간 네트워크)에 부차적인 피해 유발.
8) 국익을 위협하는 감시 활동. NSA 는 미국의 정치적 이익에 피해 유발. 미국은 공격적인 감시 프로그램으로 미국의 세계적 위상과 지위를 약화시키고 있음.
➔ 대량 감시를 위해 인터넷을 안전하지 않은 상태로 유지하면서, 경쟁 관계에 있는 다른 나라 정부나, 범죄자, 해커를 막을 수 없어 모두 위험해짐.