미국/영국 정보기관의 무차별 정보수집행위: 인터넷과 법치주의의 위기[106)]

김기창[107)]

1. 인터넷의 기술적 기초에 대한 오해: 인터넷의 '익명성'?

인터넷은 익명성이 보장되는 매체가 아니다. 고안 단계에서부터도 인터넷은 교신의 확실성과 공격에 대한 저항능력(질긴 생명력, robustness)을 확보하는데 주안점을 둔 설계 원칙(end-to-end 원칙)에 기반한 것이었을 뿐, 교신 당사자의 프라이버시나 익명성 보장이 인터넷의 기술적 특징은 아니었으며, 지금도 그렇지 않다.[108)]

인터넷의 기술적 기반을 이해하지 못하는 자들은 마치 인터넷이 '익명성'을 제공하는 교신 수단인 것처럼 전제하고 이런 저런 주장을 펴고 있지만, 웹서버나 메일서버의 로그파일을 한번이라도 들여다 본 적이 있는 사람이라면 인터넷은 교신 당사자의 행적을 이때까지의 어떠한 오프라인 교신 수단보다도 더 철저히 매순간 기록하고 있음을 쉽게 이해할 것이다. IP주소 역시, '익명성'을 보장하려는 것이 아니라, 해당 교신을 수행하는 node를 네트워크상에서 '특정'하기 위한 것이다.

암호화 기술 역시 익명성이나 개인의 프라이버시를 보장해 줄 수 있는 것이 아니다. 암호화에 사용되는 암호키를 상대방이 제3자에게 제공하거나, 제3자가 당사자들 모르게 암호키를 입수하거나, 암호 프로그램에 허점이 있거나(의도한 허점이건 의도하지 않은 허점이건), 교신내용이 거쳐 가는 여러 node 들이 모두 정직하게 자신의 임무를 수행한다는 전제가 충족되지 않는다면 암호화는 무의미하게 될 경우가 많다. 인터넷 '기술'이나 암호화 '기술'이 인간의 신뢰나 기대를 보장하거나 충족해 주는 것이 아니다. 교신 과정에 직접 간접으로 개입된 여러 당사자, 즉 '기술'이 아니라 '인간'이 자신의 임무나 약속을 지키는지가 신뢰의 핵심을 이룬다.

신뢰는 기계나 기술에 근거하는 것이 아니라, 인간의 행위와 노력에서 생겨나고 인간의 행위에 좌우되는 것이며, 기술이나 기계는 이렇

106) 이 글은 국가인권위원회의 2013년 인권단체협력사업의 지원을 받아 망중립성 이용자 포럼이 2014년 발간하는 『인터넷거버넌스를 말하다』라는 책에 실릴 예정입니다.

107) 변호사, 법학박사, 고려대학교 법학전문대학원 교수, 사단법인 오픈넷 비상임 이사, keechang.kim@gmail.com

108) RFC1958 ("Architectural Principles of the Internet") http://www.ietf.org/rfc/rfc1958.txt RFC3724 ("The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture") http://www.ietf.org/rfc/rfc3724.txt 참조.

게 생겨난 신뢰를 – 인간이 원하는 경우, 그리고 원하는 동안에만 – 겨우 '유지'해 줄 수 있는데 그친다는 평범한 진리는 현대 정보통신 기술의 현란한 복잡성에 가려서 잊혀지는 경우가 잦다. 미국과 영국의 정보기관들에 의하여 자행된 대량 정보수집행위의 일단이 조금씩 드러나면서 우리는 그동안 잊고 있었던 바로 이 평범한 진리를 다시 마주하게 된 것이다.

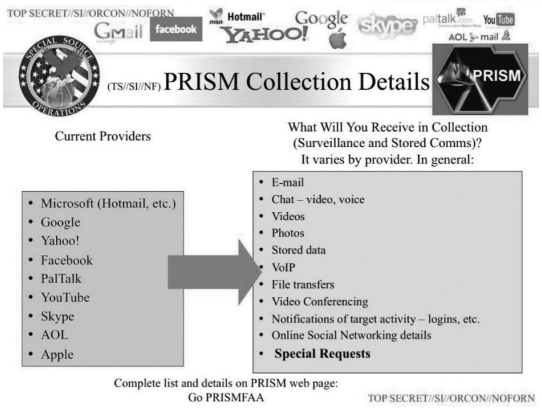
2. 미국/영국 정보기관의 대규모 정보수집행위

2013년 여름부터 영국 가디언 신문사는 미국 정보기관(NSA; 국가안보국)과 영국 정보기관(GCHQ; 교신정보총국)이 사람들이 흔히 상상하는 수준을 훨씬 넘어서는 규모로 인터넷 통신망, 통신관련 업체 등을 통하여 정보를 수집, 저장하고 있다는 내용의 보도를 하기 시작하였다. 같은 내용을 확인하고, 그 전모를 더 상세히 밝히는 후속보도는 가디언뿐 아니라 뉴욕타임즈, 워싱턴 포스트 등 여타의 언론 매체들에서도 이어졌다. 이들 보도는 미국 국가안보국 협력업체 직원이었던 에드워드 스노든이 확보하여 언론사와 공유한 자료에 기초한 것이다.

지금까지 드러난 정보 수집행위의 방대한 규모와 대담한 방법을 지극히 간단하게 소개하자면 다음과 같다.

1) 광케이블을 통한 정보 수집(Upstream collection): 미국의 국가안보국은 대량 데이터를 처리하는 광케이블망을 관리하는 업체들로부터 데이터를 확보하는 프로그램을 가동하고 있었다(Blarney, Fairview, Oakstar 그리고 Stormbrew 라는 코드네임으로 비밀리에 운영해 온 프로그램). 영국의 교신정보총국 역시 이와 유사한 대량정보 수집프로그램을 Tempora 라는 코드네임으로 운영해 오고 있었다. 미국과 영국의 정보기관들은 이렇게 각각 수집한 정보들을 서로 공유하는 관계였다.

2) 인터넷 사업자를 통한 정보 수집(Downstream collection): 미국 국가안보국은 마이크로소프트, 구글, 페이스북, 애플, 야후, 스카이프 등 미국의 인터넷 기업들로부터 이메일, 사진, 사회관계망, 접속이력, 인터넷음성통화내용, 파일 등을 입수하는 프로그램을 Prism 이라는 코드네임으로 운영하고 있다.[109]

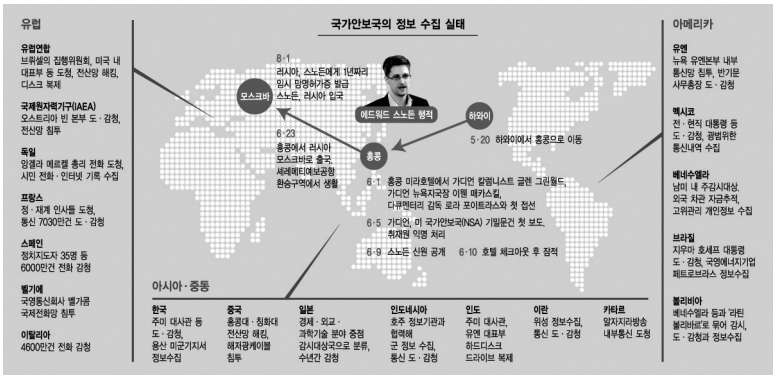


▲ 그림9) 미국 NSA가 운영한 PRISM 프로그램

109) http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/3 참조.

3) 암호화기술 무력화를 위한 활동: 미국과 영국의 정보기관은 막대한 예산을 투입하여 현재 광범하게 사용되는 암호화 알고리즘이나, 암호화 프로그램의 취약점을 공략하는 기술적 가능성을 연구, 개발하여 이미 일부 확보하고 있는 것으로 보인다. 암호화 기술의 허점을 연구하는 행위 자체는 전적으로 정당하고 바람직한 것이지만, 그 성과를 비밀에 붙이고 기존의 암호화 기술을 은밀하게 무력화하는 행위는 – 그 행위가 어떤 용도에 사용되는지 여부에 따라서 – 부도덕하고 파렴치한 것으로 평가될 수 있다. 강력한 암호화 제품이 아예 시장에 나오지 못하도록 하는 행위도 정보당국에 의하여 자행되었다. 미국 국가안보국은 보안기술업체들이 개발, 판매하는 제품들이 "허술하게 되도록 몰래 영향력을 행사"하기 위한 목적으로 연간 2억5천만 달러를 쓰고 있는 것으로 드러났다. 널리 사용되는 상용 암호프로그램에 은밀한 허점(백도어)이 포함되도록 하는 것도 바로 이 예산이 지출되는 이유 중 하나이다.[110]

대서양 횡단 광케이블이나 태평양 횡단 광케이블 등을 포함한 망 자체에 대한 접근을 통하여 입수한 데이터(암호화된 형태)에 대하여 은밀히 확보한 복호화 기술을 적용하여 그 내용까지를 파악하는 것이 가능한 수준에 도달해 있으므로, 미국과 영국의 정보기관이 원하기만 하면 지구상의 거의 모든 교신 내용을 파악할 수 있다는 결론도 무리한 것이 아니다. 일부 보도에 따르면, 지금까지 드러난 도청, 감청 행위는 적대국은 물론이고, 우호국의 수반, 주요 국제기구의 수장 등의 교신 내용까지를 대상으로 이루어졌음을 알 수 있다.[111]



▲ 그림10) 미국 NSA의 정보 수집 실태

3. 유명무실한 '사법적' 통제

광케이블을 통한 정보수집이나 인터넷 사업자를 통한 정보 수집은 흔히 해외정보감시법(Foreign Intelligence Surveillance Act; FISA)이 정한 절차에 따라서 발부된 정보수집허가서에 기하여 이루어진 것으로 보인다. 이 절차는 전통적인 영장주의를 배제하고 해외정보감시법정(FISA court)이라는 곳에서 일방주의, 비밀주의에 근거한 매우 간단한 '심사'를 거쳐서 이루어지는 것이다. 즉, 감시 대상이 될 당사자는 정보 수집이 자신에 대하여 이루어지는지 자체를 알 수도 없고, 모든 절차는 비밀리에 진행되며,

110) http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security 참조.
111) http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201311102314415

정보수집허가가 발부되었는지 여부조차도 비밀에 붙이도록 되어 있다. 이러한 내용의 법 개정은 9.11 테러 사건의 여파로 도입된 것이다.

물론 해외정보감시법에 따른 정보의 수집은 주로 외국인을 상대로 하는 것이긴 하지만, 미국 국가안보국은 영국 정보기관이 수집한 정보(미국 국민에 대한 정보까지 포함)를 공유하는 처지였으므로 내국인/외국인 구분에 따른 적법절차의 차등적 적용이라는 원칙도 사실은 무의미하게 된 경우가 많다. 해외정보감시법정의 심사 절차 자체도 지극히 형식적이고 기계적인 것이어서 사실상 어떠한 실효성도 없다는 것이 일반적인 인식이다.

사생활에 대한 광범한 침투를 쉽게 허용하는 내용의 법 개정은 9.11사태 이후에 부각된 이른바 '테러와의 전쟁' 이라는 시대적 분위기에서 도입된 것이다. 테러에 대한 '공포'와 테러 방지 수단을 확보할 '필요'를 내세워 도입된 이러한 느슨한 사법적 통제를 이용하여 대규모로 이루어진 정보 수집 행위가 테러 시도를 사전에 포착하고 방지하는데 과연 어느 정도 기여했는지는 대단히 불분명하다. 반면에 시민들에 대한 무차별적인 감시체제가 이러한 제도적 변화를 계기로 확고히 자리잡게 되었다는 점은 의문의 여지가 없이 명백하다.

테러행위가 공동체 구성원들의 자유와 생존을 위협하는 것이라는 점은 의문의 여지가 없다. 그러나 테러 대응, 국가 안보 등을 빌미로 도입되는 여러 제도들이 공동체 구성원의 자유를 심각하게 박탈한다면 그러한 제도는 그것으로 지키려는 소중한 것을 스스로 파괴하는 모순을 저지르는 것이라고 할 수 밖에 없다. 국가 안보를 내세우는 이들이 늘상 내세우는 "Salus populi est suprema lex (인민의 안녕이 지상의 법이다)" 라는 키케로의 말에 대하여 영국의 빙험 대법관은 그 오용과 남용을 경계하면서, "안보를 자유보다 우선하는 자는 어느 것도 누릴 자격이 없다" (Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety)는 벤자민 프랭클린의 말에 분명히 힘을 실어주고 있다.[112]

9.11 사태 이후, 테러와의 전쟁이라는 명분으로 도입된 '대폭 완화된 사법적 심사를 통한 사적 통신에 대한 접근' 이 지금껏 과연 실효성이 있었는지를 냉정히 재평가해야 할 시점에 도달하였다고 생각한다. 만일 이러한 대량 정보수집 및 감시행위가 실제로는 별 실효성이 없었다면 우리 모두는 득보다는 실이 많은 제도 변화의 피해자가 될 것이다. 특히 기술적 진보에 근거하여 이러한 정보입수행위가 이루어지고 있으므로, 정작 테러를 기획하는 세력들은 이러한 기술적 정보입수행위를 '우회'하는 손쉬운 다른 교신 방법이나 기법을 이미 채택하고 있을 가능성 또한 심각하게 고민해야 한다. 정작 제어, 감시되어야 할 자들에 대해서는 별 실효성도 없고, 나머지 절대 다수의 선량한 시민들은 무차별적인 사적 정보 노출을 감수하며 살아가야 한다면 지금의 상황은 개선이 필요하다.

112) 톰 빙험, 법의 지배 (김기창 옮김), 역자 후기 참조.

4. 교훈 및 대처방향

⑴ 기술적 가능성과 규범적 금지의 상관관계

종래의 교신 기술 상황에서 사생활의 자유나 통신의 비밀이 유지되었던 이유는 타인의 교신이나 활동에 대한 접근이 '기술적으로 불가능' 해서가 아니다. 예를 들어, 편지봉투에 밀봉되어 배달되는 편지의 내용을 당사자 몰래 파악하는 것이 '기술적으로 어려워서' 편지봉투를 열지 못한 것이 아니다. 유선 전화의 내용을 도청하는 것이 기술적 어려움을 제기하였던 것도 아니다. 기술적으로 가능하다고 해서, 규범적으로 그 행위를 해도 무방한 것은 아니다. 사생활의 비밀이나 프라이버시는 애초부터 기술적으로 방어되고 유지되어 왔던 것이 아니라, 규범적 금지를 준수함으로써 유지, 보호될 수 있었던 것이다.

이러한 원리는 현대의 교신 기술 상황에서도 변함없이 관철되어야 한다. 중요한 차이점은 종래의 교신 기술 상황에서는 광범한 대상(당사자들)에 대하여 그들의 교신 내용에 접근하려면 훨씬 많은 인적, 물적 자원이 소유되었던 것에 반하여, 현재의 교신 기술 속성상 무수한 사람들의 교신이 집중되어 처리되고 있으므로 그 내용에 접근하는 것이 기술적으로 오히려 쉬워졌다는 점이다. 바로 이러한 '기술적 용이함' 이 존재하는 현재에는 사적 교신에 대한 무단 접근을 규범적으로 통제해야 할 더욱 큰 필요성이 생겨났다는 점을 분명히 이해할 필요가 있다. 9.11 사태 이후에 이루어진 일은 정반대 방향으로 제도가 수정된 것이고, 그 결과를 이제 우리들이 접하게 된 것이다.

⑵ 인터넷의 기술적 속성에 대한 이해 및 계몽의 필요성

인터넷이 교신의 비밀이나 익명성을 기술적으로 보장해 줄 수는 없다는 너무나 당연하고 초보적인 사실을 더욱 널리 계몽하고, 바람직한 이용행태를 교육하는 것이 필요하다. 인터넷 망을 통하여 이루어지는 이메일, SNS, 전화 등 대부분의 의사소통 행위들이 기술적으로는 제3자에게 투명하게 그리고 완전하게 노출될 수 있음을 모든 유저들이 보다 명확하게 이해하는 것이 필요하다. 자신이 사용하는 매체의 기술적 속성을 보다 정확하게 이해하는 것이 자신의 사생활이나 프라이버시가 부당하게 침해될 가능성을 그나마 조금이라도 줄이거나 일부라도 회피하는데 도움이 된다.

그리고 소스가 공개되지 않은 상용 소프트웨어(소스가 공개되지 않으므로, 어떤 취약점이 은밀히 내재하는지를 누구도 확인할 수 없는 소프트웨어)는 가급적 사용을 피하고, 소스가 투명하게 공개된 소프트웨어를 사용하는 것이 자신의 안전과 이익에 도움이 된다는 점도 보다 널리 알릴 필요가 있다. 정보당국이 은밀히 심어놓은 숨은 취약점은 악의적인 공격자 역시도 발견하여 이를 은밀히 이용할 수 있다. 정보당국은 자신의 정보수집 필요성만을 고려에 두고 취약점을 은밀히 심어두는 결정을 할 뿐, 유저가 그러한 취약점 때문에 제3자에 의하여 공격을 당할 가능성에 대해서는 어떠한 고려나 고민, 보호도 제공하지 않는다.

⑶ 사적 교신의 비밀 보장과 공권력 행사의 투명성

상상을 초월한 규모의 대량 정보수집 행위에 직면하고, 인터넷의 속성 자체가 애초부터 이러한 정보수집행위를 기술적으로 가능하게 한다는 점을 비로소 인식할 경우, 사생활의 자유, 교신의 비밀, 프라이버시 보호는 변화된 기술 환경에서 현실적으로 아예 '기대할 수 없는 것'으로 치부하고 패배주의에 빠질 우려가 없지 않다. 그러나 이러한 시각은 잘못된 것이다. 교신의 비밀 보장, 프라이버시 보호 등은 기술적 가능성에 좌우 되는 것이 아니라, 인간의 행위에 대한 규범적 통제에 달려있다는 점을 상기할 필요가 있다. 정부의 권한 행사가 보다 투명하게 되고, 정보기관의 정보수집 신청에 대한 실효성 있는 사법적 심사가 이루어진다면, 대규모 정보수집이 비록 '기술적으로는 가능'하더라도, 실제로 지금처럼 광범하게 자행될 수는 없게 될 것으로 기대할 수 있다.

⑷ 국제적 대응의 필요

인터넷을 통한 교신, 그리고 그 교신에 대한 은밀한 접근 및 정보 수집은 어느 한 국가의 법제도만의 문제가 아니라 국제적 대응이 필요한 사안이다. 미국의 정보기관이 영국의 정보기관과 협정을 체결하고 정보 수집 행위의 결과를 공유해 온 사례에서 보듯이 정보수집 단계의 '국제공조'가 이루어져 왔는바, 이러한 행위가 가능한 것과 마찬가지로 정보수집에 대한 사법적 통제나 감시 메커니즘 역시 국제적 공조가 가능할 뿐 아니라 필요한 분야임이 분명해졌다. 따라서 각국 정부는 정보수집의 원칙, 정보수집 시도에 대한 사법적 통제의 원칙 등에 대해서 구체적인 내용과 절차에 대한 합의점을 도출하고 향후 이러한 일이 재발하지 않도록 하는데 필요한 국제적 공조 체제를 수립할 필요가 있다.

사생활의 자유, 통신의 비밀, 프라이버시 보호 등은 문명사회를 지탱하는 중요한 초석이다. 스노든의 폭로행위로 드러난 미국과 영국 정보기관의 다양한 정보수집 행위는 이러한 근본 가치들에 대한 심각한 도전으로 받아들여질 여지도 많다. 이 사태를 계기로 위와 같은 논점들에 대한 더욱 활발한 논의가 이루어 질 수 있기를 바란다.

ABSTRACT

Massive Surveillance by US-UK intelligence services : Crisis of the Internet and the Rule of Law

Keechang Kim[113)]

The revelations made possible by Edward Snowden, a contractor of the US intelligence service NSA, are a sobering reminder that the Internet is not an 'anonymous' means of communication. In fact, the Internet has never been conceived with anonymity in mind. If anything, the Internet and networking technologies provide far more detailed and traceable information about where, when, with whom we communicate. The content of the communication can also be made available to third parties who obtain encryption keys or have the means of exploiting vulnerabilities (either by design or by oversight) of encryption software. Irrebuttable evidence has emerged that the US and the UK intelligence services have had an indiscriminate access to the meta-data of communications and, in some cases, the content of the communications in the name of security and protection of the public. The conventional means of judicial scrutiny of such an access turned out to be ineffectual.

The most alarming attitude of the public and some politicians is "If you have nothing to hide, you need not be concerned." Where individuals have nothing to hide, intelligence services have no business in the first place to have a peek. If the public espouses the groundless assumption that State organs are benevolent ("they will have a look only to find out whether there are probable grounds to form a reasonable suspicion"), then the achievements of several hundred years of struggle to have the constitutional guarantees against invasion into privacy and liberty will quickly evaporate.

This is an opportune moment to review some of the basic points about the protection of privacy and freedom of individuals. First, if one should hold a view that security can override liberty, one is most likely to lose both liberty and security. Civilized societies have developed the rule of law as the least damaging and most practicable arrangement to strike a balance between security and liberty. Whether

113) Professor at Korea University Law School, Director (non-executive), OpenNet Korea

we wish to give up the rule of law in the name of security requires a thorough scrutiny and an informed decision of the body politic. It is not a decision which can secretly be made in a closed chamber. Second, protection of privacy has always depended on human being's compliance with the rules rather than technical guarantees or robustness of technical means. It is easy to tear apart an envelope and have a look inside. It was, and still is, the normative prohibition (and our compliance) which provided us with protection of privacy. The same applies to electronic communications. With sufficient resources, surreptitiously undermining technical means of protecting privacy (such as encryption) is certainly 'possible'. But that does not mean that it is permissible. Third, although the Internet is clearly not an 'anonymous' means of communication, many users have a 'false sense of anonymity' which make them more vulnerable to prying eyes. More effort should be made to educate the general public about the technical nature of the Internet and encourage them to adopt user behaviour which is mindful of the possibilities of unwanted surveillance. Fourth, the US and the UK intelligence services have demonstrated that an international cooperation is possible and worked well in running the mechanism of massive surveillance and infiltration into data which travels globally. If that is possible, it should equally be possible to put in place a global mechanism of judicial scrutiny over a global attempt at surveillance.