한국경호경비학회 – 제29호(2011): 301–336
투고일 2011. 10. 31, 심사일 2011. 11. 15, 게재확정일 2011. 12. 23

SNS(Social Network Service)의 위험성 및 Policing(경찰활동)에 미칠 영향에 대한 시론적 연구

최 진 혁

SNS(Social Network Service)의 위험성 및 Policing(경찰활동)에 미칠 영향에 대한 시론적 연구*

최 진 혁**

〈요 약〉

이 논문은 최근 전 세계적으로 확산되어 다양한 분야에서 폭넓게 사용되고 있는 Social Network Service(SNS)가 오히려 사이버 범죄나 산업스파이 등과 같은 각종 불법적 행위에 악용되고 있는 상황에 즈음하여, 특히 SNS가 가지는 보안상 취약성으로 인한 위험뿐만 아니라 기업의 기밀정보 · 핵심기술이나 개인정보 유출, 프라이버시 침해, 신원 절도(ID Theft), 타인 정보의 오 · 남용, 지적재산권 침해 및 관련 법적 문제, 범죄 증거 및 수사자료 활용, 아동 포르노 등 성범죄에의 악용, 온라인상에서의 집단 따돌림(On-line Bullying) 등 각종 사회 · 경제적 우려가 중대하고 심지어는 테러나 사회적 파장이 큰 범죄의 목표 또는 수단이 되기도 하는 등 그 잠재적 위험성이 매우 크다는 점에 주목하였다. 사실상 국내 뿐 아니라 해외에서도 SNS의 위험성이나 Policing(경찰활동)에 미칠 영향 등과 관련한 연구가 거의 전무한 형국인지라 이에 SNS에 대한 위험성의 인식과 Policing 측면에서의 적극적인 검토와 대응이 시급히 요청되고 있는 실정임을 반영하여 이 논문을 통해 SNS의 잠재적 위험성에 대한 이론적 분석과 같은 학술적인 측면뿐만 아니라 경찰활동에 미칠 수 있는 영향에 대한 실무 · 실용적 관점에서 접근의 필요성을 인지하여 탐색적 연구를 시도하였다.

주제어 : 소셜 네트워크 서비스, 위험성, 경찰활동, 보안, 취약성, 사이버 범죄, 프라이버시

---

* 이 논문은 연구자가 『한국행정학회』 하계학술대회(2011. 6. 24)에서 발표하였던 내용을 수정 · 보완하여 최종 완성한 것이며, 2011학년도 대전대학교 신진교수 연구 장려금에 의해 지원되었음.

** 대전대학교 사회과학대학 경찰학과 교수 / 한국기업보안협의회 회장.

목 차

Ⅰ. 들어가며

최근 "소셜 네트워크 서비스(Social Network Service: 이하 'SNS')"[1]가 전 세계적으로 확산되면서 국내에서도 이제 매우 익숙한 용어가 되었다. 폭발적으로 증가한 인터넷(Internet) 이용자와 급속도로 빨라진 네트워크(Network) 및 와이파이(Wi-Fi)와 같은 무선통신망의 확충, 그리고 스마트폰(Smartphone)[2] 사용자층의 확산 등에 기인하여 국내에서도 SNS 이용자들이 엄청나게 빠른 속도로 증가하였을 뿐만 아니라 일상화된 양상을 보이고 있는 추세인지라 바야흐로 한국 사회에서도 'SNS 전성시대'라는 표현이 이제는 전혀 낯설지 않은 실정이다.

언론 등에서 종종 접할 수 있듯이 국내 일부 정치인과 유명 연예인 및 스포츠 스타는 물론, 기업 최고경영진도 트위터(Twitter)[3][4]나 페이스북(Facebook)[5] 등과 같은

1) Social Network Service(SNS)의 구체적인 개념 정의에 관하여는 후술되는 "Ⅱ. 이론적 배경" 본문에서 설명하는 내용 참조.

2) 일반적인 피쳐폰(Feature Phone: 저사양/저성능 휴대전화)에 비하여 보다 향상되고 진보된 컴퓨팅 역량과 연결성(Connectivity)을 제공하는 휴대전화를 통칭하여 이르는 말로서, 가장 단순화된 표현으로 비유하자면 카메라폰과 PDA(Personal Digital Assistant: 휴대정보단말기)의 기능들을 결합해놓은 휴대전화라고 할 수 있겠다(연구자 註 & 참고자료: Wikipedia).

3) 트위터(Twitter)는 미국 트위터사(Twitter Inc.)가 운영하는 웹사이트 서비스로서 소셜 네트워킹(Social Networking) 및 마이크로 블로그(Micro-blogging) 서비스를 제공한다. 트위터는 2006년 3월 잭 도시(Jack Dorsey), 비즈 스톤(Biz Stone) 및 에반 윌리엄스(Evan Williams)에 의해 최초로 개설되어 2007년 50만 3천 명, 2009년 5천 8백만 명, 그리고 2011년 12월 현재 3억여 명 이상의 사용자를 확보하고 있으며, 2010년 10월의 뉴욕타임즈지 분석기사에 의할 경우 2010년 4월 이후 매일

SNS를 상당수 활용하고 있고, 국내 굴지의 대기업들도 자사 브랜드(Brand)와 제품 홍보 및 소비자들과의 원활한 커뮤니케이션(Communication)을 위해 적극적으로 도입·활용하고 있는 추세다. 예컨대, 2010년 국내 모 통신사의 경우 국내의 모바일(Mobile) SNS 시장을 선도하려는 시도로 세계 최대 SNS 사업자인 페이스북과 포괄적 협력 제휴를 선언[6]하기도 했다.

21세기 지식정보화 사회는 디지털(Digital)·모바일·유비쿼터스(Ubiquitous) 시대로 불리어질 만큼 정보통신 분야 기술의 비약적 발전과 더불어 초고속 정보통신망에 의해 전 세계가 하나로 연결되고 사회 모든 분야에서 엄청난 양의 정보가 디지털화되고 있는 한편, 인터넷 이용의 급증은 각종 정보를 교류·저장·처리하는 역량을 극대화시켰을 뿐 아니라 온라인(On-line) 및 오프라인(Off-line) 상에서 수집 가능한 단편적인 정보들을 상호 연결함으로써 특정한 개인 또는 사건에 관한 완전한 정보로 가공하여 활용할 수 있는 기술적인 기반(Tool)을 제공하고 있다. 이러한 기술적인 진보와 인터넷 인프라(Infrastructure)의 확산으로 인하여 개인정보는 본인들이 인식하지 못하는

평균 37만여 명의 신규 사용자가 등록되고 있는 추세이다(자료: (1) 미국 트위터사 홈페이지(http://twitter.com), (2) BBC 뉴스(http://www.bbc.co.uk/news/business-12889048), (3) The New York Times(뉴욕타임즈), "Why Twitter's C.E.O. Demoted Himself," http://www.nytimes.com/2010/10/31/technology /31ev.html?_r=2&pagewanted=1&partner=rss&emc=rss (2010. 10. 30) 기사 참조).

4) 트위터는 블로그(Blog)의 인터페이스(Interface)와 미니 홈페이지(Mini Homepage)의 '친구 맺기' 기능, 그리고 메신저(Messenger)의 신속성 등을 함께 모아 제공하는 SNS이다. 트위터 사용자들은 '트윗(Tweets)'이라고 불리우는 텍스트(Text) 기반 메시지(Message) 형식의 포스트(Post)를 통해 소통하는데, 한 번에 쓸 수 있는 글자 수는 "최대 140자"로 제한되어 있다. 웹(Web)에 직접 접속하지 않더라도 스마트폰과 같은 휴대기기 등의 다양한 방법을 통하여 글을 올리거나 받아볼 수가 있으며, 트윗에 덧글("Reply")을 달거나 또는 '리트윗(Retweet)' 기능을 사용해서 특정 글을 다른 사용자들에게 퍼트릴 수도 있다. 또한 관심 있는 상대방을 뒤따르는 '팔로우(Follow)', 곧 '팔로워(Follower)'로 등록할 수 있는 기능도 제공한다. 이와 같이 언제 어디서나 정보를 실시간으로 교류하는 '빠른 소통'이 가장 큰 특징인 트위터는 '신속한 정보 유통망'으로 각광받고 있다(자료: (1) 트위터사 홈페이지 제공 정보(http://twitter.com/about) (2) BBC 뉴스(http://www.bbc.co.uk/news/business-12889048), (3) Wikipedia (http://en.wikipedia.org/wiki/Twitter), 2010년 11월 1일 검색).

5) 페이스북(Facebook)은 2011년 12월 현재 8억여 명이 넘는 사용자--Facebook 홈페이지 통계자료 참조(http://www.facebook.com/press/info.php?statistics, 2011년 6월 12일 검색)--를 확보하고 있는 세계 최대의 SNS 웹사이트로서 2004년 2월 당시 미국 하버드대(Harvard University) 재학 중이던 마크 주커버그(Mark Zuckerberg) 등이 설립하였다. 2010년도 세계 인구를 기준으로 환산하면 세계인 14명 중 한 명 꼴로 페이스북을 이용하고 있는 것이다.

6) 자료: 아이뉴스 24 (2010. 11. 3), "SNS가 통신 잡아먹는(?) 세상", http://itnews.inews24.com/php/newsview.php?g_serial=525948&gmenu=020300 (2010. 11. 3 검색).

사이에 끊임없이 누군가에 의해 수집·저장되거나 심지어는 불법행위 등에 오·남용될 여지가 다분하다고 보아도 과언이 아닐 것이다(이창범·김본미, 2004).

이처럼 특히 온라인상으로 정보가 교환·저장·처리되는 사이버(Cyber) 세계의 특징과 SNS가 가지는 '교류' 및 '공유'의 특성은 그 수많은 사용자 수와 온라인상에 저장되어 있거나 접근 가능한 방대한 규모의 정보들이 제공하는 이익 또는 이점과 결합함으로써 SNS가 원래 추구·제시하려던 목적과 다른 역기능을 생산하는 결과를 초래하고 있는 상황이다. 예컨대, 페이스북의 경우 5억여 명의 사용자가 한 달 평균 117억 시간을 페이스북 상에서 소진하고 매월 300억 건의 컨텐츠(Contents)[7]가 공유되며, 트위터의 경우에도 하루에 1억 9천만여 건의 트윗(Tweet)이 생성[8]되고 있는 바, 이러한 엄청난 규모의 사용자 수와 그들 간의 상호작용, 그리고 그 과정에서 생성·교류·저장되는 컨텐츠나 개인정보 등은 현대 범죄의 중요한 표적이 되기 마련인 것이다.

이와 같이 SNS가 오히려 사이버 범죄자들은 물론 산업스파이 등의 표적이 되거나 또는 각종 불법적 행위에 오·남용되거나 악용되고 있는 현상이 지속적으로 도출되고 있는 상황이다. 특히, SNS가 가지는 보안상의 취약성으로 인한 위험--해킹(Hacking), 피싱(Phishing)[9], 스팸(Spamming·Spam Mails) 등--뿐만 아니라, 기업 기밀정보·핵심기술 및 개인정보의 유출, 프라이버시(Privacy) 침해, 신원 절도(ID Theft), 타인 정보의 오·남용, 지적재산권 침해 및 관련 법적 문제, 범죄 증거 및 수사자료로의 활용, 아동 포르노 등 성범죄에의 악용, 트롤링(Trolling)[10], 온라인상 집단 따돌림

7) 인터넷이나 컴퓨터 통신 등을 통하여 제공되는 각종 정보나 그 내용물—자료: 네이버 백과사전(http://100.naver.com/)--을 지칭하는 말이나, 페이스북의 경우 웹페이지(Webpage), 웹 링크(Web links), 뉴스기사, 블로그 포스트, 노트, 사진 앨범 등을 통칭하여 사용하고 있다(연구자 註).

8) Facebook 홈페이지 통계자료(http://www.facebook.com/press/info.php?statistics) 및 트위터사 제공 정보(http://twitter.com/about) 참조 – 2011년 6월 10일 검색.

9) 피싱(Phishing)이란 금융기관 등의 웹사이트나 또는 거기서 보내온 메일로 위장하여 불특정 다수에게 메일을 발송해 위장된 홈페이지로 접속하도록 한 뒤 인터넷 이용자들의 계정정보(아이디 및 암호: ID & Password), 인증번호, 신용카드 정보, 계좌 정보 등의 금융정보를 획득하여 불법적인 목적으로 사용하는 일종의 사기 수법으로서, 인터넷 보안상의 기술적 취약성을 공략하거나 이용자들을 기망하는 사회공학(Social Engineering) 기법 중 하나이다(자료: (1) Microsoft Corporation. "What is social engineering?", http://www.microsoft.com/protect/yourself/phishing/engineering. mspx, (2) Wikipedia(http://en.wikipedia.org/), (3) 네이버 백과사전(http://100.naver.com/)).

10) 온라인상의 커뮤니티(Community)에서 사용자(참여자)들을 감정적으로 자극하거나 또는 정상적인 토론을 방해하려는 목적으로 선동적이거나 주제와는 전혀 무관한 메시지를 게시하는 행위 등을 말한다(연구자 註).

(On-line Bullying) 등 개인 차원을 넘어서 각종 사회·경제적 우려가 중대하고, 심지어는 테러나 사회적 파장이 큰 범죄의 목표 또는 수단이 되기도 하는 등 그 잠재적 위험성이 매우 크다고 하겠다.

그러나 SNS에 대한 위험성의 인식과 Policing(경찰활동) 측면에서의 적극적인 검토와 대응이 시급히 요청되고 있는 형국임에도 국내뿐 아니라 해외에서도 SNS의 위험성 또는 경찰활동에 미치는 영향 등과 관련한 연구가 거의 전무한 실정이고, 기존의 국내 학술연구로 SNS와 관련한 마케팅 전략, 웹 2.0, UCC(User Created Contents)[11] 활용, 사용자 만족 정도, 사회자본 형성, 비즈니스 모델, 서비스 동향 및 전망, 사회문화 경향(Trend) 등에 치중한 소수의 사례가 있을 뿐인 관계로 SNS의 잠재적 위험성에 대한 이론적 분석과 같은 학술적인 측면뿐만 아니라 Policing(경찰활동)에 미칠 수 있는 영향에 대한 실무·실용적 관점에서 접근의 필요성을 인지하여 이에 탐색적 연구를 시도하였다.

Ⅱ. 이론적 배경

1. SNS(Social Network Service)

1) SNS의 정의

SNS(Social Network Service: 소셜 네트워크 서비스)란 사회적 관계의 형성 개념을 인터넷 공간으로 가져온 것으로서, 개인이 온라인(인터넷) 상에서 친구와 같은 특정한 관계를 맺고, 정보를 공유하며 지속적으로 커뮤니케이션을 확대해나가는 일련의 커뮤니티(Community) 구성 활동을 아우르는 말이다.[12] 사실상 SNS 자체가 21세기에

11) UCC(User Created Contents)는 사용자가 직접 제작한 컨텐츠(사진, 동영상, 번역물, 게시물 등의 모든 개인 저작물 포함)를 의미하는 신조어를 일컫는다(연구자 註).

12) 간혹 학자에 따라서는 '온라인 커뮤니티 서비스(On-line Community Service)'를 SNS의 범주에 포함시키기도 하나 온라인 커뮤니티 서비스는 집단중심적(Group-centered)인데 비해 SNS는 개인중심적(Individual-centered) 개념이라는 차이가 있다(자료: (1) Boyd, D. M. & Ellison, N. B. (2007), "Social Network Sites: Definition, History, and Scholarship," Journal of Computer- Mediated Communication, 13(1)(http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html) 및 (2) Wikipedia(http://en.wikipedia.org/wiki/Social_network_service) - 2010. 11. 1 검색)).

들어 생성된 신개념인 관계로 이에 대한 명확하고 통일된 정의는 아직 찾아보기 어려우나, 이 연구에서는 앞서 간략히 설명한 내용과 다음 <표 1>에서 정리한 바를 토대로 SNS에 대한 개념을 "인터넷 상에서 개인들이 정보를 공유하고, 의사소통하거나, 인적 관계(네트워크)를 형성하는 것을 돕는 서비스"로 정의하여 사용하기로 한다.

미국 UC 버클리대(University of California-Berkeley)의 다나 보이드(Danah M. Boyd) 교수 및 미시간 주립대(Michigan State University)의 니콜 엘리슨(Nicole B. Ellison) 교수는 SNS를 다음과 같이 정의하고 있다. 보이드와 엘리슨 교수에 의하면 SNS는 "개인(이용자)들로 하여금 (1) [인터넷 상의 특정한 SNS와 같이] 한정된 체계(System) 내에서 공개적이거나 반공개적인 자신의 프로파일을 구성하고, (2) 인적 연계(Connection)를 공유하는 타 이용자들의 목록(명단)을 표출하며, (3) 자신의 연계 목록 및 동 체계에서 다른 이용자들에 의해 생성된 연계 목록을 열람하거나 관계를 맺을 수 있도록 하는 웹 기반 서비스이며, 이러한 연계의 성격과 명칭은 SNS 사이트마다 각기 다를 수 있다"고 설명하고 있다.[13)]

〈표 1〉 SNS에 대한 정의

출 처	정 의	자료 웹페이지(URL)
Britanica 백과사전	개인들이 메시지를 교환하고, 정보를 공유하며, 때로는 공동의 활동(Joint Activities)에 있어 협력 · 협업하기 위한 온라인상의 커뮤니티	http://www.britannica.com/EBchecked/topic/1335211/social-network?anchor=ref1073083
Wikipedia (위키피디아)	개인들 간에 사회적 관계(네트워크)를 형성하거나 나타내는데 중점을 둔 온라인 사이트로서, 인적 네트워크 내에서 생각(사상), 활동, 사건, 관심사 등에 관한 정보를 공유할 수 있도록 하는 서비스	http://en.wikipedia.org/wiki/Social_network_service
네이버 백과사전	인터넷 상에서 친구 · 선후배 · 동료 등 기존 지인(知人)과의 인맥 관계를 강화시키고 또 새로운 인맥을 쌓으며 폭넓은 인적 네트워크--인간관계--를 형성할 수 있도록 해주는 서비스로서, 인터넷에서 개인의 정보를 공유할 수 있게 하고 의사소통을 도와주는 1인 미디어 또는 1인 커뮤니티	http://100.naver.com/100.nhn?docid=922657

13) Boyd, D. M. and Ellison, N. B.(2007), Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), Article 11 (http://jcmc.indiana.edu/vol13/ issue1/boyd.ellison.html).

〈표 2〉 SNS 유사 용어[14)]

유사 용어	개념 및 내용
Social Network	'Social Network(소셜 네트워크)'는 우정, 연대감, 공통적인 관심, 금융 거래, 반감, 성적 관계, 신앙, 지식, 명망 등과 같이 하나 혹은 그 이상의 특정 유형의 상호의존성에 의해 연결 되는 개인 또는 조직– "Nodes(교점 · 접속점)" 로 표현--으로 구성된 사회적 구조
Social Network Analysis	'Social Network Analysis(소셜 네트워크 분석)'이란 "Nodes(교점)"과 "Ties(관계)"로 구성되는 네트워크 이론(Network Theory) 관점에서 사회적 관계를 살펴보는 것으로, 때로는 조직들이 어떻게 서로 상호작용 하는지 알아보기 위해 사용되기도 함 Nodes는 네트워크 내 개인 자신을, 그리고 Ties는 개인들 간의 관계를 지칭하며, 이러한 개념들은 흔히 소셜 네트워크 다이어그램(Social Network Diagram) 상에서 Nodes는 점으로, Ties는 선으로 표시됨 가장 단순한 형태의 소셜 네트워크는 Nodes(교점) 간에 선택된 연관성 있는 관계(Ties)의 도식(Map)이며, 특정 개인이 연계되는 교점들은 그 개인의 사회적 관계(Contacts)를 표현 소셜 네트워크는 가정에서부터 국가적 수준에 이르기까지 많은 단계에서 작용하며, 문제 해결이나 조직 운영의 방법, 그리고 개인의 목표 성취 달성의 정도를 결정하는데 있어서 핵심적인 역할을 하는 것으로 기존의 학술적 연구를 통해 입증
Network Society	'Network Society(네트워크 소사이어티)'는 네덜란드의 사회학자 반 디크(Jan van Dijk)가 그의 저서 "De Netwerkmaatschappij(1991)", "The Network Society(1999 & 2006)"에서, 그리고 카스텔(Manuel Castells) 교수가 3부작 "The Information Age(1996)" 중 첫 번째인 "The Network Society"에서 명명하였고, 웰만(Barry Wellman) 교수와 힐츠 & 투로프(Roxanne Hiltz & Murray Turoff) 교수팀도 네트워크 소사이어티 개념에 관해 연구 반 디크는 네트워크 소사이어티를 사회적 및 미디어 네트워크의 결합이 사회의 주요한 조직 형태 및 모든 수준--개인적, 조직적, 사회적 단계--에 있어서 가장 중요한 구조를 형성하는 사회로 정의하면서, 집단, 조직, 그리고 커뮤니티(대중)에 의하여 형성되는 대중사회(Mass Society)와 비교 카스텔은 개인이 중심이 된 사회관계의 새로운 양태(Pattern)의 출현을 강조하며, 개인이 네트워크의 중심이 되어 타인과의 관계를 형성하는 것을 네트워크화된 개인주의로 표현 웰만은 어떠한 사회든 계층적 구조로 한정된 집단으로서 보다는 '네트워크'의 연결로 가장 잘 파악할 수 있다고 주장하면서, 개인화된 네트워크 중심의 "네트워크화된 개인주의(Networked Individualism)"를 강조하였으며, 네트워크 소사이어티의 중요한 요소로서 커뮤니티, 일(직장), 그리고 조직의 3가지에 그 초점을 맞춤 힐츠와 투로프 팀은 "The Network Nation(1978)"을 통해 '컴퓨터의 지원을 통한 커뮤니케이션은 사회를 변형시킬 수 있다'고 주장하였는바, 이는 인터넷의 출현 이전에 기술된 것으로서 선견지명을 엿볼 수 있는 부분 반 디크, 웰만, 힐츠 & 투로프, 그리고 카스텔 등에 의해 상술된 '네트워크 소사이어티'는 현대 기술을 통해 잘 나타나고 있는데, 페이스북이나 마이스페이스(MySpace) 등과 같은 웹사이트는 네트워크 소사이어티가 작용 중인 주요한 본보기라고 할 것 기타 네트워크 소사이어티와 유사한 사례로서 제임스 마틴(James Martin)은 1978년 대중매체(매스컴)과 전기통신 네트워크에 의해 연결된 사회를 지칭하는 'The Wired Society'라는 용어를 사용

14) 연구자가 Boyd, D. M. and Ellison, N. B.(2007), Social network sites: Definition, history, and scholarship. Journal of Computer–Mediated Communication, 13(1), Article 11 (http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html) 등 해외 문헌자료 및 Wikipedia, "Social Network," http://en.wikipedia.org/wiki/Social_network (2010. 10. 30 검색) 등을 참조하여 작성.

2) SNS의 특징

SNS는 '웹 2.0(Web 2.0)'[15]의 특징을 고스란히 담고 있어 '웹 2.0의 총아'로 표현되고 있기도 하는데, 최근 들어 전 세계적으로 SNS의 이용이 급증하는 이유는 바로 SNS가 내재하고 있는 웹 2.0의 중요한 특성[16]인 사용자 참여 중심의 인터넷 환경과 정보의 공유, 신규 서비스의 창출 및 집단 지성(Collective Intelligence)[17] 등과 맞물려 있다고 할 것이다. 현대 정보통신 기술의 발달과 인터넷 공간(Infrastructure)의 확산은 개인을 보다 가치 있는 존재로 만들었고, 이는 현대인의 사회적 특성과 연계되어 개인이 중심이 되는 새로운 형태의 사회관계이 출현을 목격하게 된 것이다.

정보사회 및 커뮤니케이션 분야의 저명한 이론가인 마누엘 카스텔(Manuel Castells) 교수에 의하면 웹 2.0 환경에서 인간관계의 특징을 '네트워크화된 개인주의(Networked Individualism)'에서 규명하면서, 개인이 중심이 되는 사회관계의 새로운 양태(Pattern)의 출현을 강조하고 있다. 즉, 마누엘 카스텔과 배리 웰만(Barry Wellman)[18] 교수 등은 개인의 능력이 부각됨과 더불어 개인이 네트워크의 중심이 되어 타인과의 관계를 형성하는 현상을 네트워크화된 개인주의로 표현하고 있다. 더불어 카스텔에 의하면 네트워크화된 개인주의는 고립된 개인들의 집합(Collection)이

15) 웹 2.0(Web 2.0)은 2004년 10월 팀 오라일리(Tim O'Reilly)에 의해 최초로 소개된 개념으로 기존의 웹 1.0(Web 1.0)이 인터넷 상에서 제공되는 정보나 서비스를 보기만 하고 일방적으로 수신만 하는 단순 '푸시형(Push-type)'이었던데 반해서, 누구나 손쉽게 인터넷 상에서 데이터를 생산하고 공유하면서 다양한 서비스를 생성해 낼 수 있도록 한 사용자 참여 중심의 역동적인 인터넷 환경을 말한다. 예를 들어, 유명한 브리태니카(Britanica) 온라인 백과사전이 웹 1.0이라면 위키피디아(Wikipedia)는 웹 2.0을 대표할 것이며, 또한 개인 홈페이지가 웹 1.0이라면 블로그(Blogging)는 웹 2.0에 해당한다고 하겠다(자료: (1) O'Reilly, Tim(2005), "What Is Web 2.0" (http://oreilly.com/web2/archive/what-is-web-20.html, 2005. 9. 30),
(2) Wikipedia(http://en.wikipedia.org/),
(3) 네이버 용어사전(http://terms.naver.com/item.nhn?dirId=205&docId=25362)).

16) 웹 2.0의 특성으로는 플랫폼(Platform)으로서의 웹 환경 지향, 사용자의 직접 참여, 새로운 서비스의 창출(창조성), 정보의 공유(분산화), 그리고 '집단 지성(Collective Intelligence)' 또는 '협업 지성(Collective Intelligence)' 등이 강조된다.

17) 집단 지성(Collective Intelligence)이란 다수의 개체들이 서로 협력 또는 경쟁하는 과정에서 획득한 지적 능력의 산물로서 얻어진 집단의 지적 역량을 일컫는 말로서 협업 지성(協業 知性)과 같은 의미이다. 집단 지성의 대표적 사례로는 웹 2.0과 Wikipedia(위키피디아) 등을 들 수 있는데, 이는 지식이나 정보의 생산자 또는 수혜자가 따로 없이 누구나 생성 가능하고 모두가 손쉽게 공유하면서도 지속적으로 진보하는 집단 지성의 특성을 잘 보여주고 있다(자료: (1) Wikipedia(http://en.wikipedia.org/wiki/Collective_intelligence), 2010. 11. 1 검색, (2) 네이버 백과사전 (http://100.naver.com/100.nhn?docid=8548 25)).

18) Wellman, Barry, et al.(2003), "The Social Affordances of the Internet for Networked Individualism," Journal of Computer-Mediated Communication, 8(3).

아니라 사회적 유형(Social Pattern)의 하나라는 것이다.[19] 따라서, 개인들의 온라인상에서의 상호작용은 전체 사회 조직에도 영향을 미치게 되며, 이러한 네트워크화된 개인주의적 특징을 고스란히 포함하고 있는 것이 바로 SNS라고 하겠다.

2. '위험성'에 관한 고찰

21세기 지식정보화 사회에 있어서의 위험(Risk)은 과거와는 그 종류뿐만 아니라 규모의 측면에서 사뭇 다르며, 또한 그러한 위험의 영향과 잠재력은 현대사회의 가장 두드러진 특징 중 하나라고 할 것이다. 이와 관련, 독일의 저명한 사회학자인 울리히 벡(Ulrich Beck)은 이러한 사회를 "위험사회(Risikogesellschaft; Risk Society)"라는 관점에서 접근하였다. 벡은 사회 변동과 '위험사회'의 개념 형성에 큰 영향을 미쳤는데, 벡의 주장에 따르면 사회는 전통적·전근대적 사회(Traditional/Pre-modern Society)에서 초기 단순 근대사회(Early-Simple Modern Society)로, 그리고 다시 "성찰적 근대성(Reflexive Modernity)"을 근저로 한 위험사회(Risk Society)로 전이된다고 설명하고 있다.[20]

벡에 의하면 전통적 산업사회에서는 부를 생산하는 논리가 위험을 생산하는 논리를 지배--부를 위해 위험을 감수--했다면 위험사회에서는 이 관계가 역전된다는 것이 그의 논점이다. 벡은 위험사회론을 통해 사회 전반에 걸친 위험(성)에 대하여 논하면서 그 대안으로 '성찰적 근대성'을 제시하였는데, 이것은 전통적 산업사회의 핵심 요소였던 부의 분배를 안전과 위험--또는 안전과 위험의 분배--이라는 새로운 개념으로 바꿔야 한다는 것, 즉 근대성을 새롭게 재구성해야 한다고 주장한 것이다.[21] 이는 위험의 요인이 정확히 밝혀져야만 위험한 것이 아니라 사회현상이 복잡다단해지고 또 과학기술이 급속하게 발달하면서 인간이 인지하지 못하는 위험들은 주위에 수없이 도사리고 있으므로 가시적 위험이 아니라는 이유로 간과한다면 그 위험은 더욱 축적되거나 확대되어 결국 막대한 피해를 입히게 될 것[22]이라는 근저에서이다.

---

19) Manuel Castells(2003), The Internet Galaxy: Reflections on the Internet, Business, and Society, Oxford: Oxford University Press, pp. 129-132.

20) "A Summary of Ulrich Beck - Risk Society: Towards a New Modernity" (http://www.nextreformation.com/wp-admin/resources/risk-society.pdf).

21) Beck, Ulrich(1992) Risk Society: Towards a New Modernity. London: Sage.

22) 그렇지만 벡(1992)은 위험사회에 있어서의 위험성은 일반인의 시야에는 잘 띄지가 않기 때문에 전문가 집단에 의존해야 하지만 그러한 전문가가 없거나 부족한 현실에 있어서 위험(성)에 대한

특히, 벡이 현대 위험사회의 성찰적 근대성에서 강조하고 있는 요소들 중 과학기술의 발달 및 의사소통(Communications), 정보사회(Information Society), 사회기술적 네트워크(Socio-technical Network), 개인(Individualization 혹은 Individualism)의 강조, 집단적 구조(Structure & Institutions => We)로부터 '자율성'(Self as the Primary Agent => Autonomous)으로의 전이, 고객(개인) 중심의 공동생산(Client-center Co-production), 그리고 지식 기반(Knowledge-based) 등은 SNS가 내재하고 있는 특성과 밀접하게 연관되는 것으로서 벡이 위험사회의 요소로서 제시[23]하였음은 상당히 주지하여 볼 만하다.

한편, 한국사회에서의 위험을 유형화 한 이 재열 외(2005)의 연구[24]에 의하면 위험의 유형을 지구적 생태 위험, 자연적 재해 위험, 국가적 안보 위험, 건강 상 위험, 경제적 생계 위험, 사회적 해체 위험, 그리고 기술적 재난 위험의 7가지로 분류[25]하고 있는데, 여기서 과학기술은 그 발전으로 생산성과 생활의 편의를 증대시키는 놀라운 생산력의 원천인 동시에 살상과 같은 막대한 사회적 재난을 야기하는 원천으로서 보았다. 특히, 기술적 재난의 위험은 현대 정보화 기술의 발달에 편승하여 새로운 차원의 위험으로서 전이되고 있는 실정이며, 이는 벡이 주목한 위험사회의 핵심적 위험인 현대 과학기술의 위험과도 일맥상통한다고 하겠다.

즉, 국가의 행정이 정보통신시스템을 중심으로 실행되고 사회가 재편성되면서 기업이나 조직 일부의 문제가 전 사회적 위기로 급속히 확산되거나 또는 위험이 전면화될 가능성이 커지게 되었고, 아울러 개인정보의 광범위한 노출과 프라이버시에 대한 위협 역시 크게 증가하였는바, 이러한 점에서 SNS가 가지는 위험성은 결코 개인 차원에서 머무르거나 혹은 위험의 정도가 적다고 할 수는 없을 것이다.

인식은 자연과학, 인문 및 예술을 망라한 전문가 집단과 시민사회, 그리고 이해관계와 현실 간의 새로운 만남에 의해 결정되며, 그러한 결정에는 학제 간, 시민집단, 기업, 그리고 정부의 끊임없는 협상과 열린 논의의 과정이 필요할 것이라고 보았다.

23) Jarvis, Darryl S. L.(2010), Theorizing Risk: Ulrich Beck, Globalization and the Rise of the Risk Society, National University of Singapore.

24) 이 재열 외(2005), 사회안전지표 개발을 위한 국민 안전의식 조사, 소방방재청, pp. 58–62.

25) 이 재열 외(2004)의 이전 연구보고 "위험사회와 생태적 · 사회적 안전(정보통신정책연구원)"에서는 '건강 상 위험' 대신에 '정치적 억압 위험'으로 분류하고 있다.

3. 선행연구 검토

1) 탐색적 연구의 필요성

이 연구는 SNS의 내재적 특성과 잠재적 위험성을 중심으로 한 이론적 고찰을 통해 보안상의 취약성과 사회적 위험·위협에 대해 분석하고 특히 경찰활동에 미칠 수 있는 영향을 중심으로 연구함으로써 SNS를 이용한 국가기밀·산업기술의 유출 시도나 개인정보·프라이버시 및 지적재산권 침해, 테러나 각종 범죄에의 악용, 기타 발생 가능한 위험요소에 보다 효과적이고 적절하게 대처할 수 있는 방안도 모색해 보려는데 그 목적을 두었다. 더불어 민간영역 및 공공부문에서 바람직한 SNS 위험관리 대책의 마련을 위한 정책적 제언을 제시하려는 데에도 그 연구의 필요성이 있었다.

하지만, 기존 연구 및 문헌자료에 대한 검토를 시도하였으나 SNS와 관련한 마케팅 전략, 웹 2.0, UCC 활용, 사용자 만족 정도, 사회자본 형성, 비즈니스 모델, 서비스 동향 및 전망, 사회문화적 트렌드 등에 치중한 소수의 사례가 있을 뿐 사실상 SNS의 위험성이나 경찰활동에 미치는 영향 등에 관한 국내 선행연구가 전무하며, 해외의 경우에도 직접적으로 연계되는 사례가 거의 없는 실정인 관계로 연구자는 미국과 유럽 등을 중심으로 2000년대 이후의 유사 분야 연구사례와 학술자료에 대한 폭넓고 집중적인 조사·분석을 통하여 시론적 연구를 시도하였다.

2) 선행연구 고찰

먼저 해외의 선행연구를 검토해본 바, SNS와 관련한 프라이버시 침해 가능성 또는 그로 인한 잠재적 위험성에 관한 연구 사례가 대표적이었다. Gross & Acquisti(2005)는 미국 카네기 멜론대(Carnegie Mellon University) 재학생 중 페이스북 사용자 4천명을 대상으로 페이스북 프로파일(Profile)을 분석하여 학생들에 의한 게시 자료나 개인정보 중 프로파일에서 흔히 발견되는 고향이나 생년월일 등과 같은 정보를 활용하여 해당 사용자의 사회보장번호(Social Security Number)--한국의 주민등록번호--를 재구성해낼 수 있는지 여부 등 잠재적인 프라이버시 침해 가능성을 검토하였다.

또한 Acquisti & Gross(2006)의 후속 연구에 의하면 프라이버시 보호를 위한 학생들의 욕구와 그들의 실제 행동 간에는 괴리(Disconnection)가 존재한다고 주장하였는데, Stutzman(2006)의 페이스북 사용자 조사 및 Barnes(2006)의 "프라이버시 역설

(Privacy Paradox)"[26] 역시도 유사한 주제의 선행연구 사례라고 하겠다. 특히, Barnes(2006)는 10대들이 '인터넷의 공공적 특성(Public Nature)'을 잘 인식하지 못할 때 프라이버시의 역설이 일어난다고 설명하였다. 또한 Utz & Kramer(2009)는 SNS 사이트에서의 프라이버시 역설을 사용자 개인의 특성과 집단규범을 중심으로 재해석하였다.

다음으로 SNS 사이트와 사용자 신뢰관계를 분석한 연구로서 Dwyer, Hiltz, and Passerini(2007)는 SNS 이용자들의 서비스 제공 웹사이트에 대한 신뢰 정도가 공유하려는 정보--정보의 양--에도 영향을 미친다고 주장하였다. 그들의 연구 결과 페이스북 이용자들이 마이스페이스(MySpace) 이용자들에 비해 자신들이 사용하는 사이트(페이스북)에 대한 신뢰를 더 표시했으며, 이는 동 사이트에서 정보를 더욱 많이 공유하려는 의향을 표출한 것이라고 분석하고 있다.

SNS 사용자의 보안의식과 관련하여 Jagatic, Johnson, Jakobsson, and Menczer(2007)는 SNS 사이트들로부터 자유로이 접근 가능한 프로파일을 이용하여 마치 네트워크 상의 친구에게서 온 것처럼 보이도록 조작하는 피싱(Phishing) 기법을 활용하여 SNS 이용자들이 낯선 사람은 아니지만 '조작된 친구'에게 정보를 주는지 여부를 확인하려는 연구를 수행하였다. Jagatic 등은 그들의 "Social Network Phishing and Control Experiment(소셜 네트워크 피싱 및 통제 실험)" 연구를 통해 성별 간의 차이나 조작된 피싱 피해를 당한 사람들의 반응 등 다양한 실험적 분석을 시도하였다.

또한 사용자 보안의식 관련 설문조사 결과 미국 내 십대들이 온라인상에서의 잠재적 프라이버시 침해 위협을 인식하고 있고, 상당수가 그러한 잠재적 위험을 줄이기 위해 적극적인 조치를 취하고 있는 것으로 나타나 긍정적 관점을 도출하였다. Pew에 의하면 55%의 십대들이 온라인상에서 프로파일을 가지고 있지만 그 중 66%가 모든 인터넷 사용자들에게 '공개'로 설정해 놓지는 않았다고 응답(Lenhart & Madden, 2007)하였고, 자신의 온라인 프로파일을 모두에게 공개(개방)하였다고 응답한 십대 중에서도 46%가 프로파일 상의 정보 중 적어도 일부는 허위로 게시한 것이라고 응답하였다.

SNS 상에서의 프라이버시에 대한 사용자의 통제 및 인식과 관련하여 Preibusch,

26) "프라이버시 역설(Privacy Paradox)"이란 한편으로는 프라이버시가 침해될까 염려하면서도 실제로는 페이스북과 같은 SNS에 가입하기 위해 개인정보를 제공하고 또 많은 정보를 페이스북 프로파일이나 온라인상에서 게시 · 공유하는 등 모순되는 행태를 보이는 것을 말한다(연구자 註).

Hoser, Gürses, and Berendt(2007)는 SNS 사이트에 의해 제공되는 프라이버시 옵션이 이용자들로 하여금 프라이버시에 대한 인식 또는 관점의 차가 있는 '친구'들과의 갈등을 조절·조정할 수 있는 유연성을 제공해주지 못하는 문제가 있다고 주장하였다. 이와 같은 갈등 문제를 해결하기 위한 방안으로 Preibusch 등은 SNS에 있어서 프라이버시 준거 틀(Framework)을 마련할 것을 제안하였다. 그 외에도 Boyd & Ellison(2007)은 SNS의 특징을 설명하고 포괄적인 개념적 정의를 제안하는 한편, SNS의 역사적 측면에서의 성찰 및 변천·발달 과정 등에 관한 학술적인 분석을 시도하였다.

한편, 국내의 SNS 관련 문헌자료 추이를 살펴본 바, 기존의 국내 학술연구는 앞에서 언급한 바 있듯이 SNS와 관련한 마케팅 전략, 웹 2.0, 사용자 만족도, 비즈니스 모델, 서비스 동향 등에 치중하여 비교적 소수의 자료가 존재하나, 그 중 이 연구에서 검토한 사례로는 이 형효 외(2009)의 "SNS 환경의 아이덴티티 공유 및 보호에 관한 연구" 등이 있다. 이 형효 외(2009)는 SNS 사이트를 통해 공유되는 아이덴티티(Identity)가 웹 2.0 환경에서 사용자 편리성과 업무 효율성을 제고할 수 있는 서비스 시나리오에 대해 Mockup(모형) SNS 사이트를 중심으로 구현하려 시도하였으나, 사례 제시에 치중한 반면 아이덴티티 소유자에 의한 사용 통제 및 프라이버시 보호 측면에서의 고려에 대해서는 소홀한 부분을 노출하고 있는 것으로 판단된다.

Ⅲ. SNS의 위험성 및 영향

1. SNS의 내재적 위험

SNS는 네트워크상에서 사람들을 만나고, 친구를 사귀며, 유사한 개인적 또는 사업적 이해를 교류하고, 정보를 공유하는 좋은 장소나 기회를 제공하는 등 잠재적으로 유용한 사업상 도구 또는 개인 홍보를 위한 전략적 매체[27]일 수 있으나 이는 사용자들이 평소 충분한 주의를 기울이고 상식 및 합리성이라는 준거기준에 근거해서 활용할 때만 가능하다고 생각해야 할 것이다. SNS는 사용자 및 소속 기업·기관·조직에 보안상의 심각한 위협이나 개인정보 탈취, 프라이버시 침해, 기타 법적 책임 문제를 야기할 수 있다.

27) Edwards, John(2007), "The Security Risks of Social Networks" (2007-7-9).

Brenner(2009)에 의하면 SNS는 7가지 치명적 위험성[28]을 내재하고 있다고 하였는데, 여기에는 개인정보나 소속 기업·조직 내부정보의 지나친 공유, 개인적 이해·관심사와 기업 또는 공적 활동과의 혼동, 패스워드 변경 태만 및 관리 소홀, SNS에의 과도한 몰입, 가장 많은 조회 수 또는 팔로워(Follower)를 기록하는데 매진, 무작정 클릭(Click)하게 되는 경향, 사용자 자신뿐만 아니라 타인까지도 위험에 노출시키는 결과 초래 등이 있다. Kelleher(2009) 역시 SNS로 인한 위험요소로 바이러스 및 악성코드, 사회공학(Social Engineering)[29] 위험성, 법적 책임, 개인 또는 기업 평판(Reputation) 악화 문제, 생산성의 하락, 기업 또는 조직 구성원 사기 저하, [Bandwidth(네트워크 대역폭) 등과 같은] 내부자원(Internal Resources)에의 악영향 등을 제시[30]하였다.

2. 보안상의 위협 및 취약성

Sophos(2010)의 "2010년도 보안위협보고서(2010 Security Threat Report)"에 의하면 최근에 현안으로 대두되고 있는 보안상의 위협과 관련하여 특징적인 현상으로 범죄자들이 SNS 사이트상에서--자택이든 직장이든 상관없이--잠재적 피해자를 물색하여 공격한다면서 그 위험성을 제기하였다. Sophos는 많은 SNS 웹사이트가 자신들의 시장점유율 확보 및 성장에만 치중하는 반면, 기존 고객(이용자)들을 현존하는 인터넷상의 보안 위협으로부터 적절히 보호하는 것에는 소홀하다고 지적하고 있다.

SNS 사용자들을 대상으로 한 Sophos의 2010년도 조사 결과에 의하면 SNS 중에서 '페이스북'이 가장 보안상의 위험이 크다고 인식하고 있는 것으로 나타났는데, 페이스북이 전체 응답자 중 60%, 마이스페이스가 18%, 트위터가 17%, 그리고 구인·구직 전문 SNS인 LinkedIn(링크드인)이 4%를 차지하였다. 비록 LinkedIn이 다른 상위 3개 SNS에 비해 비교적 덜 위험한 것으로 인식하고 있기는 하나 여전히 해커들로부터의 정보 탈취의 위험은 상존하고 있다고 할 것이며, 특히 LinkedIn과 같은 인적 네트워크 형성 위주의 소위 '인맥 맞춤형' SNS의 경우 구인·구직 활동에 많이 활용되므로 해커들이 기업이나 부서의 구성도, 직원명, 직위 체계 등 조직도를 효과적으로 빼내기 쉬

28) Brenner, Bill(2009), www.csoonline.com (2009-6-30).
29) 인터넷 보안상의 기술적 취약성을 공략하거나 이용자들을 기망하는 기법을 통칭한다(연구자 註).
30) Kelleher, David(2009), "Information Management Special Reports" (2009-10-6).

운 경로를 제공하고 있기 때문에 실질적인 위험성은 훨씬 높다고 보아야 한다.[31]

한편, Sophos의 2010년도 조사 결과 57%의 SNS 이용자들이 SNS를 통해 스팸메일(Spam Mail)을 받았다고 응답하였는데 이는 전년(2009년) 대비 70.6% 상승한 수치로 나타났고, 36%의 이용자들이 SNS를 통해서 악성코드(Malicious Code)를 받은 경험이 있다고 응답하였는데 이는 전년 대비 69.8% 상승한 수치였다. 또한 조사 대상 기업의 72%가 임직원들의 SNS 사용이 보안 및 기업 경영 측면에서 위험을 야기할 것이라고 판단되어 걱정하고 있다고 응답하였으나, 조사 대상 기업 중 49%가 임직원들의 SNS 접속이나 사용에 어떠한 제약도 현재 가하지 않고 있다고 응답하여 상당히 우려되는 실상을 표출하고 있었다.[32]

3. 사이버범죄 공격 경로로 이용

페이스북이나 트위터와 같은 SNS를 대상으로 한 해킹의 우려가 날로 증가[33]하는 등 SNS가 각종 사이버범죄의 공격 경로로 악용되는 현상이 가시화되고 있다. 2009년도에 이미 트위터에서 짧은 주소 서비스를 통해 악성코드를 유포한 사례가 있었고, 최근에는 스마트폰의 급속한 보급과 함께 다양한 SNS 애플리케이션이 등장함에 따라 개인정보를 노린 해킹이 증가할 것으로 보인다. 또한 SNS 사이트상에서 본인 확인이 어려운 점을 악용해 유명인을 사칭하거나 유명인의 SNS 계정을 탈취하여 범죄 등에 악용할 수도 있으며, SNS 서비스 제공업체(웹사이트)를 직접 겨냥한 해킹도 발생할 것으로 판단된다.[34]

대표적 사례로서 "Clampi 악성코드(Trojan.Win32.Clampi.513024)"의 경우 주로 SNS나 메신저를 통해서 전파되는데, 국내에는 2009년 9월 21일 최초 발견되었으며 영어권 국가의 은행이 주된 표적이었다. Clampi 악성코드는 SNS 또는 메신저 사용자가 금융사이트에 접속해서 인터넷 뱅킹을 시도할 때 로그인(Login) 정보를 가로채가는 특화된 악성코드로서, 이 악성코드에 감염되면 'iexplore.exe'를 실행시켜 CPU 리

31) 참고자료: http://ivebeenmugged.typepad.com/my_weblog/2010/02/social-networks-risk.html?cid=6a00e008d035db8834013488112f38970c.

32) Sophos(2010), "Security Threat Report 2010"(http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf).

33) AhnLab(안철수연구소)이 2010년 1월에 발표한 연례 최대 보안 Issue 12가지를 살펴보면 "SNS를 이용한 공격 확산"이 제시되어 있다.

34) AhnLab(2010), "2010년 이슈가 될 보안 위협 12가지" (2010. 1. 12).

소스를 많이 사용하게 되고 사용자가 금융사이트에 접속하는지를 모니터링 후 금융정보를 갈취하게 된다. 실제로 Clampi 악성코드로 인해 ID 또는 패스워드 등 개인정보가 노출되어 금융거래 범죄에 이용된 경우가 다수 발생하였다.[35]

SNS를 통한 악성코드 유포는 주로 해외 제공 서비스인 페이스북이나 트위터 등을 중심으로 이루어졌으나, 국내 사용자가 대다수를 차지하는 SNS인 N사의 '미투데이(me2day)'를 대상으로 악성코드가 유포된 사례도 발생하였음은 주목할 필요가 있겠다. 이는 Windows 업데이트 파일로 위장한 악성 DDL(Data Definition Language: 데이터 정의어) 파일이 트위터 및 국내 기업의 SNS인 미투데이를 통해 추가 악성코드를 다운로드하면서 '좀비 PC(Zombie PC)'를 양산하는 역할을 수행한 경우이다. 동 사례에서 악성코드는 감염된 PC를 좀비 PC로 만들어 공격자(해커)의 추가 공격 명령을 기다리도록 설계되었던 것이다.[36]

또한 페이스북 쪽지를 통해서 유포되는 악성코드 사례도 발생하였는데, 2010년 9월 AhnLab은 페이스북 쪽지로 악성코드를 유포하는 [인터넷상의 파일 주소인] 단축 URL (Uniform/Universal Resource Locator)이 전달되고 있다고 경고하였는데, 이는 2010년 8월 초부터 영국 등지에서 유포된 형태와 유사하며 국내에서는 처음으로 대량 유포된 것이었다고 한다. 동 악성코드는 페이스북 쪽지를 통해 'Aloha' ':-D' 'Hello' 등 메시지와 함께 단축 URL이 전달되는데, 이 URL을 클릭 후 코덱(Codec)으로 가장된 프로그램(setup902674.exe)을 설치하면 'Windows Security Alert'라는 가짜 백신 파일이 잇달아 다운로드 되면서 해당 사용자의 페이스북 계정에 등록된 친구들에게도 동일한 메시지가 전파[37]되어 피해를 광범위하게 확산시키는 것이다.

4. 프라이버시 침해 문제

SNS 사용자 입장에서는 다음 3가지의 주요한 프라이버시 침해 위험성이 상존하고 있다고 하겠다. 그것은 SNS에 의한 또는 SNS를 활용한 전체적인 [개인]정보의 획득·인지, 범죄자나 범법 행위자에게의 정보 전달, 그리고 사용자 자신의 신원 관련 정보에 대한 통제성 상실 등이다. SNS 업체(웹사이트)는 그들의 포털(Portal) 상에

35) Hauri(2010), http://hauri.co.kr/customer/security/virus_view.html?intSeq=1774&page=1&keyfield=&key=&SelectPart=1.
36) YTN 경제(2010), http://www.ytn.co.kr/_ln/0102_201007230906428225.
37) AhnLab 뉴스(2010), http://blog.ahnlab.com/ahnlab/948.

서 사용자들 및 마케팅 파트너들이 행하는 모든 행위를 추적하거나 확인할 수 있으며, 사용자들과 관련된 엄청난 양의 2차적 개인정보 수집이 가능할 뿐 아니라, 심지어 사용자들의 사전 동의나 고지 없이도 정보의 수집이 가능하게 되어 있다.

따라서 SNS 상에서 제공되거나 유통 및 배포되는 수많은 신원 관련 [개인]정보는 손쉽게 범죄자들에게 입수되며, 또한 범죄자들은 SNS에게 위탁된 정보들을 악용하여 잠재적 피해자들--범행 대상--을 골라내거나 연락하기 위한 참고 데이터로 활용하는 것이 가능한 것이다. 즉, SNS 상에서의 사용자 프로파일 정보와 더불어 사용자에 대한 접촉(연락)의 간편성과 용이함은 범죄자들 입장에서는 SNS가 매우 유용한 범죄도구(Platform)로 활용될 수 있다고 하겠다.

뿐만 아니라 SNS는 그 생래적 특성 상 스토킹(Stalking), 온라인에서의 집단 따돌림(On-line/Cyber-Bullying), 명예훼손 및 모욕(Libel & Slander), 트롤링(Trolling)[38] 등과 같이 프라이버시와 연계되는 사이버 범죄에 흔히 악용될 소지가 다분하다. SNS 웹사이트의 정보들은 특정 사용자의 명성이나 평판에 쉽게 손상을 가하도록 사용될 수도 있으며, SNS 상에 노출된 수많은 귀속정보들은 특정 사용자뿐만 아니라 제3자의 신원을 절취하는데 필요한 정보로 별 어려움 없이 역분석·역추리(Reverse Engineering) 할 수 있는 위험성이 존재하는 것이다.

무엇보다 심각하게 생각해야 할 점은 SNS 사용자들은 자신들의 [개인]정보라고 할지라도 일단 SNS 웹사이트 상에 게시한 이상 포괄적 동의를 SNS 사업자 측에 제공한 것이며, 그러한 정보들에 대한 SNS 사업자의 제2차적 사용에 관해서도 동의한 것으로 간주되므로 현실적으로는 해당 정보들에 대한 통제성을 상실하는 것과 동일한 결과를 가져오게 된다는 사실이다. 이로 인해 비단 프라이버시의 침해뿐만 아니라 기업이나 공공기관의 기밀정보나 핵심기술 등도 누설·유출될 수 있는 위험성이 상존하고 있다는 것을 유념해야만 하겠다.

5. 정보 유출 및 ID Theft(신원 절도)

전 세계적으로 가장 많은 사용자를 확보하고 있는 페이스북의 경우 해킹 또는 위

38) 각주 10) 참조: 온라인상의 커뮤니티(Community)에서 사용자(참여자)들을 감정적으로 자극하거나 또는 정상적 토론을 방해하려는 목적으로 선동적이거나 주제와는 전혀 무관한 메시지를 게시하는 행위 등을 말한다(연구자 註).

조 계정(Impersonated or Fake Account)에 의한 신원 절도(ID Theft) 및 개인정보 유출 사건이 종종 보고되고 있는 실정이다. 가장 대표적 예로 2010년 7월 28일 세계 각 국 페이스북 사용자—당시 5억여 명--중 무려 5분의 2에 육박하는 1억 7천만여 명의 개인정보 파일이 단 한 명의 해커에 의해 DB(데이터베이스)로 공개되어 온라인상에 사용자 정보가 노출되는 사건이 발생하여 SNS 웹사이트나 서비스 제공자가 보유·관리하는 사용자 개인정보의 악용 우려에 대한 논란이 제기되기도 했었다.

테크크런치(TechCrunch)에 의하면 보안전문가인 론 보우즈(Ron Bowes)가 페이스북 온라인 디렉토리로부터 사용자 정보를 추출, 토렌트(Torrent)로 컴파일링해 자신의 홈페이지에 업로드 했다고 보고하였다. 테크크런치가 전한 바에 따르면, 론 보우즈가 추출한 사용자 정보에는 프로파일로 연결되는 URL(Uniform Resource Locator)과 각 사용자의 성명, 주소와 전화번호까지 적혀 있고, 전체 용량은 2.8GB에 이르며, 심지어 그가 사용한 프로그램들까지 업로드 되어 있었는바, 이 프로그램들은 해커라면 손쉽게 사용할 수 있는 프로그램인 것으로 알려져 그 문제의 심각성을 더욱 증폭시켰다[39].

또한 2008년에 최초 탐지되어 2009년 이후 유명했던 “Koobface” 바이러스[40]의 경우 페이스북 사용자를 주 대상으로 한 것으로 피해 사용자의 PC를 감염시켜 궁극적으로는 패스워드와 같은 계정정보, 신용카드 번호, 기타 개인정보를 탈취해내는 것이 목표로 알려지고 있었다. Koobface 바이러스는 공격 대상 PC 시스템을 감염시켜서 해당 PC 내의 정보를 마음대로 검색하고 수집할 수 있게 만드는 것으로서, Koobface 바이러스를 통해 일단 탈취해낸 정보는 해커나 범죄자들에 의해 타인의 신원을 가장한 후 또 다른 범법행위를 자행하거나 혹은 피해자의 재정적인 손실을 야기하는 등 전반적으로 심각한 폐해를 유발하였다.

최근에 ENISA(The European Network and Information Security Agency: 유럽 네트워크 및 정보보안 기구)에서 발표한 보고서에 의하면 스마트폰 등 휴대폰을 통한

39) 자료: (1) TechCrunch(2010), http://techcrunch.com/2010/07/28/hacker-proves-facebooks-public-data-is-public/, (2) Blotter by 강명훈(2010. 7. 30), http://www.blotter.net/archives/35918.

40) Koobface 바이러스는 2008년 12월 최초 탐지되어 2009년 3월에 보다 강력한 버전이 출현하였는데, 이 바이러스는 이미 감염된 SNS(페이스북) 사용자의 ‘친구’들에게 메시지를 보내는 방법으로 전파되며 메시지를 받는 사용자가 첨부된 실행 파일을 Adobe Flash Player 업데이트로 믿고 다운로드 하는 순간 대상 PC 시스템을 감염시켜 해당 PC 내의 정보를 마음대로 검색하고 수집할 수 있게 만드는 바이러스이다(연구자 註).

SNS 접속·사용 시 위험성과 위협의 종류에 대해 설명하면서, 특히 신원 절도, 개인이나 기업 명성(평판)에 대한 중대한 침해, 정보 유출 등에 중점을 두고 모바일 상에서의 위험성과 위협에 대처하고 안전한 SNS 사용을 위한 17가지의 황금률(Golden Rule)을 제시하고 있다. 동 보고서에 따르면 유럽 내 조사 대상 17개국 2억 8천 3백만 명 중 2억 1천 1백만 명이 SNS를 사용하며, 그 중 6천 5백만 명 이상의 이용자들이 모바일 기기를 사용해서 페이스북과 같은 SNS에 접속하는 것으로 나타났다.[41]

ENISA 보고서에서 연구된 대표적 신원 절도 사례로는 이탈리아 튜린대(Univeristy of Turin) 교수의 가짜 페이스북 계정을 만들어 그의 명성(평판)을 해치는 악성 내용을 게시한 경우를, 그리고 정보 유출 및 기업 명성(평판)에 대한 중대한 침해의 사례로는 자사 항공기 및 그 승객들의 청결상태를 비난하는 글을 페이스북에 올린 13명의 직원을 해고한 버진 아틀란틱(Virgin Atlantic) 항공사의 예를 들고 있다. 나아가 동 보고서는 정보보호와 관련한 유럽 규준(European Directive on Data Protection "Dir. 95/46/EC") 관점에서 SNS 세상에 대한 종합적이고 포괄적인 시각을 제시한다.[42]

SNS 관련 개인정보 유출 및 신원 절도 사례 중 놀라운 것은 로널드 노블(Ronald K. Noble) 인터폴(Interpol) 사무총장의 경우이다. 노블 인터폴 사무총장은 2010년 9월 17일 홍콩에서 개최된 제1회 인터폴 정보보안 컨프런스 참석 후 자신의 페이스북 계정 2개가 신원 절도 당한 사실을 알게 되었다고 한다. 동 사건과 관련하여 영국 데일리 메일(Daily Mail)의 인터넷판 보도(2010. 9. 20)에 따르면 노블 사무총장은 페이스북에 자기 명의로 두 개의 허위 계정이 만들어진 것을 인터폴 사무총국(본부) 내 보안사고대응팀(Interpol's Security Incident Response Team)에서 최초로 발견했다고 전하고 있다.

6. 테러 및 중범죄에의 악용

2010년 9월 노블 인터폴 사무총장은 자신의 페이스북 계정 신원 절도 사실을 알게 된 후 가진 인터뷰에서 테러리스트들이 금융정보 등을 훔치기 위해서 해킹하는 사이버 범죄자와 유사한 방법을 사용할 수 있다고 경고하면서 "사이버 범죄가 매우 현실적인 위협으로 떠올랐으며, 사이버 공간의 익명성을 고려하면 이는 지금까지 우리가

41) Source: ENSIA(2010), "Onkline as soon as it happens."
42) Baltic IT&T News(2011), "Forum Baltic IT&T 2011" (2011. 6. 20).

직면한 가장 위험한 범죄 중 하나"라고 언급하는 한편, "한 나라의 전력망 혹은 은행 시스템에 대한 공격이 초래할 충격적인 결과를 상상해 보라"고 전언하였다고 한다.[43]

이 사건과 관련, 영국 데일리 메일에 의하면 페이스북 내 노블 사무총장 명의의 위장 계정 개설자 중 한 명은 이를 인터폴의 "Operation Infra-Red 2010"[44] 작전과 관련하여 도피 중인 범죄 용의자 정보를 입수하는데 이용했다고 밝혔다고 한다. 동 사례는 SNS를 이용하는 사이버 범죄의 심각성과 더불어 중범죄자·조직범죄단 또는 테러리스트들에 의한 사이버 공격이 상당히 지능적이면서도 상상을 초월하는 중대한 결과를 초래할 수도 있음을 경고해주는 사례라고 할 것이다.

한편, 2010년 미국 Fox News 보도에 의하면 일주일 간 자체 취재 및 조사 결과 페이스북의 홈페이지가 아동 포르노(Child Pornography)에 고스란히 노출되어 있다고 보도하면서 페이스북이 아동들을 대상으로 한 음란물을 제대로 차단하지 못하였다는 비판을 제기하였다. Fox News는 페이스북이 미국 국립 미아 및 학대 아동 방지 센터(NCMEC)에서 아동 착취와 관련된 금기어(금칙어)를 자동적으로 차단하는 조치를 취하고 있다고 했지만 실제로 검색을 해 본 결과 이 같은 차단 조치에 상당한 허점이 있는 것으로 드러났다고 밝혔다.

이는 페이스북의 검색 창을 통해서 '아동 하드코어(Pre-Teen Hard Core)'의 약자인 'PTHC'를 입력한 결과 197명의 회원이 가입된 그룹 페이지가 검색되었고, 페이스북 측 책임자 역시 아동 포르노물이 검색된다는 사실을 확인하고 자신들의 청소년 보호 조치에 문제점이 있음을 시인하게 된 것이다.[45] 2000년대 이후 아동 관련 음란물은 전 세계적으로 문제가 증폭되고 있는 아동 성범죄의 주요한 원인으로 지목되고 있고 또 엄하게 처벌되어야만 하는 위험성 높은 범죄이므로 SNS를 통한 아동 음란물의 유통 및 확산 방지를 위해 더욱 철저한 단속과 예방적 경찰활동이 필요할 것이다.

SNS의 테러 및 중범죄에의 악용 위험성과 관련하여 최근 들어 주목해야 할 것으로 "스테가노그래피(Steganography)"가 있다. 고대 그리스어에 그 어원을 두고 있는 스테가노그래피는 암호화(Encryption)나 암호기법(Cryptography)과는 달리 통신하고자

43) Daily Mail (2010. 9. 20) & 연합뉴스, "인터폴 총장 "페이스북서 신원 도용 당해"" (2010. 9. 20).
44) "Operation Infra–Red 2010"은 국경을 넘어 장기 도피 중인 450여 명의 국제 현상수배 중범죄자 색출 및 검거를 위해 전 세계 29개국으로부터 50여 명의 전담 수사관이 파견되어 2010년 5월 3일부터 동년 7월 15일까지 실시된 인터폴(Interpol)의 대규모 작전계획을 말한다(연구자 註 / 인터폴 홈페이지: www.interpol.int).
45) Fox News(2010. 10. 21) & 연합뉴스, "페이스북, 아동 포르노물에 무방비"(2010. 10. 22).

하는 '메시지의 존재 자체를 은닉하려는 비밀통신 기법'으로서, "Covered/Protected"를 뜻하는 Steganos(στεγανός)와 "To Write"를 나타내는 Graphein(γράφειν) 또는 Graphos를 합친 단어로 이는 "Concealed/Covered Writing(은닉된 메시지 혹은 비밀통신문)"을 의미한다. 스테가노그래피는 전달하려는 기밀정보 등의 메세지를 이미지 파일 혹은 MP3와 같은 오디오 파일 등에 암호화해서 숨기는 기법이다.[46]

만약 스테가노그래피 기법을 통해 암호화된 메시지를 SNS를 활용하여 주고받을 수 있다면 테러리스트 집단에게는 실로 최상의 은닉성과 익명성을 보장하는 은밀한 통신 및 의사소통의 수단으로 기능할 수 있는 위험성을 제공하는 결과를 낳게 될 것이다. 익명을 요구하는 미국 정부 관리와 전문가들에 의하면 이미 테러리스트 집단들은 테러목표 사진 및 지도뿐만 아니라 테러 공격의 세부지시 등도 SNS, 스포츠 채팅방이나 포르노 사이트 게시판, 기타 웹사이트 서비스를 통해 숨기거나 비밀리에 교신해오고 있었다고 밝힘[47]으로써 충격을 주기도 하였다.

7. SNS와 도·감청 문제

2010년 9월 미국 행정부 및 수사·사법·보안 당국(백악관·법무부·FBI·NSC (National Security Council))이 전체 디지털 통신--페이스북, 트위터, 스카이프(Skype), 블랙베리(Blackberry) 등--에 대한 감시 및 도청 합법화 방안을 모색 중이라고 밝혀 논란이 된 적이 있었다. 동 법안의 요점은 페이스북이나 트위터 같은 SNS 및 스카이프 등과 같은 인터넷 전화 서비스 사업자를 대상으로 국가안보 및 테러 예방·대응 등의 목적을 위해 미국 수사·사법·보안 당국의 통신 도·감청을 가능케 하는 기술 도입을 의무화함으로써 사실상 모든 SNS에 대해 미국 정부가 일상적으로 감시 가능한 시스템을 만들어 전체 디지털 통신 내용을 언제든 감청하겠다는 의사의 발현이었다.

---

46) 예를 들면, 레오나르도 다 빈치의 모나리자(Mona Lisa) 그림과 같은 이미지 파일이나 최신 유행 팝송과 같은 MP3(음악) 파일에 유조선 설계도나 반도체 핵심공정 등의 정보를 특정 코드(Code)를 공유하고 있는 전달자 및 수신자를 제외하고는 어느 누구도 눈치 채지 못하도록 암호화해서 전달할 수가 있는 것이다.

47) 전직 美 FBI 국장인 루이스 프리(Louis Freeh)가 미국 상원 법사위원회에서 밝힌 바에 의하면 FBI 수사에 있어 테러리스트들이 스테가노그래피와 같은 최첨단 은닉 암호화 통신 기법을 [SNS 웹사이트 등을 통해] 사용하고 있는 것으로 의심해 왔다고 전하면서, "빈 라덴뿐만 아니라 수많은 테러 범죄자들이 최첨단 은닉 통신기술을 사용함으로 인해 수사에 어려움을 겪고 있다"고 고충을 토로하였다(자료: The Dallas Morning News, 2001-10-12).

이는 종래의 제한적 감청을 전면적 감시로 확대하겠다는 미국 정부의 의사 표시로서, 기존의 법규에서는 범죄나 테러 수사에서 해당 수사·사법당국의 도·감청을 가능하게 하기 위해 전화 및 인터넷 서비스 제공 사업자(ISP: Internet Service Provider)에 그런 시스템 정비가 요구[48]되고 있었지만 SNS의 경우는 그 대상이 아니었다.[49] 결국 국가안보상의 이유 및 테러 예방이나 대응을 위해서는 SNS를 비롯한 디지털 통신에 대한 도·감청이 불가피한 조치라는 정부 측 주장과 정보의 과도한 통제 및 사생활 침해라는 일반 시민들의 입장이 첨예하게 대립하게 되었다.

여기서 미국 정부가 추진하려는 신규 법안[50]은 SNS를 포함하는 모든 종류의 통신 서비스(페이스북·트위터 등 SNS, 스카이프와 같이 P2P(Peer to Peer) 메시징이 가능한 소프트웨어, 블랙베리와 같이 암호화된 이메일 발송 매체 등)를 대상으로 도·감청 명령이 승인될 경우 해당 기업이 이를 수행할 수 있도록 하는 내용이 그 골자이다. 이러한 배경에는 이미 전화보다 인터넷--SNS--을 사용해서 소통·통신하는 인구가 급속도로 늘어남에 따라 범죄와 테러행위 관련 정보 수집 및 예방과 검거가 날이 갈수록 어려워지고 있기 때문[51]이기도 하다.

이와 관련, 미국의 뉴욕타임즈(The New York Times)에 따르면 "동 법안은 안보상의 요구와 사생활 보호, 그리고 혁신의 촉진 사이에 어떻게 균형을 맞출 것인지에 대한 새로운 문제들을 제기하고 있다"고 보도하였다. 문제는 도·감청 기술을 SNS 제공 업체 등에 요구할 경우 오히려 해커나 사이버 범죄자 등에 의해서 악용될 수도 있는 거대한 구멍을 스스로 뚫는 것이나 다름없는 결과를 가져올 위험성[52]도 있으

48) 미국 내 전화 및 광대역망은 1994년의 '통신수단의 법 집행 협조에 관한 법(The Communications Assistance to Law Enforcement Act)'의 적용을 받는데, 미국의 수사 · 사법당국이나 요원들은 동 법에 의해 광케이블 전화시스템에서부터 디지털 네트워크 및 휴대폰 통신에 이르기까지 정부의 정보통신 감시 능력을 보장받았기에 필요 시 정보통신 서비스 업체를 통해 통신을 도 · 감청할 수 있었다(연구자 註).

49) 그러나 2000년대 이후 최근의 신생 디지털 통신 서비스 업체 모두에게 1994년의 동 법이 적용되는 것은 아닌 관계로 일부 해당되는 업체나 서비스의 경우 도 · 감청 역량을 새로 유지해야 하는 반면, 여타 업체들은 법령에 따른 도 · 감청 기술 · 체계 개발 및 유지 명령이 있지 않는 한 관망하는 자세를 보이고 있던 상황이었다(연구자 註).

50) SNS를 포함한 모든 디지털 통신 서비스 제공 업체들은 도 · 감청 및 해독 기술 · 체계를 갖추어야 하고, 해외에 서버를 두고 미국 내에서 영업하는 기업들의 경우 도 · 감청 수행이 가능한 미국 내 기지를 세워야 하며, 또한 P2P(Peer to Peer) 통신을 가능케 하는 소프트웨어 개발자들은 도 · 감청이 가능하게끔 재설계해야 한다는 내용과 더불어, 만약 이행치 않을 경우에는 벌금 및 기타 제재를 받을 수 있도록 규정하고 있다(연구자 註).

51) 미국 FBI의 비밀수사 담당 부서의 경우 2009년 한 해 동안 통신 서비스 업체들의 전자감청 역량 보조를 위해 약 1천만 달러를 지출한 것으로 보고되었다.

며, 또한 한국의 경우 국익 보호나 범죄 수사를 위한 경찰활동에 있어서 SNS 통신 영역의 도·감청 인가 범위 및 절차, 그리고 SNS 제공 업체의 공익적 책임 한계 등에 대한 법제적 검토가 선행될 필요가 있을 것이다.

Ⅳ. 논의 및 결론

이상에서 살펴본 바와 같이 SNS의 세상에서 사용자(고객)는 사실상--SNS 서비스 제공자의 입장에서 볼 때--그저 "숫자"나 "돈벌이 신호"에 불과함에도 현대 지식정보화 사회에 있어서 인터넷 인프라의 확충과 모바일 및 디지털 기술의 급속한 발달은 정치인, 정치적 이해집단, 마케팅 전문기업, 유명 인사, 또는 미래의 잠재적 고용주 등으로 하여금 SNS 웹사이트를 소위 "정보의 금광(Gold Mine of Information)"으로 탈바꿈시켜 인식하게 만들었다. 하지만 SNS는 그 서비스 개시 시점부터 보안상 고려가 충분히 반영되어 있어야 하는 바, 소셜 네트워킹(SNS) 애플리케이션(Application)들이 진보할수록 새로운 보안상의 도전에 직면하게 될 것으로 보인다.

특히 SNS 포털(Portal)과 소셜 네트워킹 애플리케이션이 더욱 많은 정보를 사용자들에게 요구할수록 사용자의 프라이버시는 감퇴될 것이며, SNS가 기치로 내세우는 유연함과 소통 및 교류의 철학은 보안 및 Policing(경찰활동) 측면에서는 오히려 사용자들로 하여금 자신뿐만 아니라 '친구들'은 물론이고 소속 기업, 기관, 조직을 보호하기 위해서 보다 더 경각심을 가져야 할 것임을 일깨워주고 있다고 하겠다. 결국 SNS에 있어서 보안상의 위협과 프라이버시 침해 등의 문제에 대한 최상의 참된 해법은 바로 "사용자의 실체에 대한 노출을 최소화(Limit Your Presence!)"하는 것이라고 할 것이다.[53]

이 연구를 통해 SNS의 특성과 내재적 위험 및 잠재적 위협 등에 대하여 고찰하는 한편, Policing(경찰활동)에 어떠한 영향을 미칠 수 있을지를 시론적으로 검토해보고

52) 자료: (1) 뉴욕타임즈(The New York Times) 인터넷판, www.nytimes.com, 2010. 9. 27, (2) 워싱턴포스트(The Washington Post), www.washingtonpost.com, 2010. 9. 28, (3) 시사큐비즘, "트위터 · 페이스북, 도 · 감청 시대 열리나" (2010. 9. 29).

53) 참고자료: (1) Collins, Brendan(2008), "Privacy and Security Issues in Social Networking", www. fastcompany.com (2008-10-3), (2) McAfee(2010), "Social Networking Apps Pose Surprising Security Challenges."

자 하였다. 먼저 SNS의 내재적 특성으로 인한 위험성과 관련해서는 경찰활동에 직접적인 부하(Workload)를 야기하거나 경찰 내부자원 관리(Police Resource Management)의 측면에서 큰 부담을 주기 보다는 기업이나 조직 내부의 문제 혹은 민사적 규제 사안에 해당될 소지가 많다고 사료된다.

그러나 SNS가 유발하는 보안상의 위협 및 취약성과 관련하여 본다면 전문 해커나 산업스파이(Economic Espionage), 정보브로커(Information Brokers), 그리고 기타 범죄자들에 의해 악용되거나 다수의 피해자가 발생할 우려가 높다고 하겠다. 심지어 국가 핵심기술이나 기업의 기밀정보 등과 같이 국익과 관련한 손실도 배제할 수는 없다고 할 것이므로 보다 적극적(Proactive)이면서도 예방적(Preventive) 행태의 경찰활동 전략 마련과 대응이 필요할 것이다.

페이스북이나 트위터 사용자의 폭증과 더불어 SNS가 각종 사이버범죄의 공격 경로로써 활용되는 현상이 지속적으로 가시화되면서 특히 악성코드 유포를 통한 금융정보의 갈취나 SNS 계정정보 탈취 위험이 날로 증가하고 있다. 21세기 디지털·모바일 시대의 특성에 비추어 볼 때 SNS로 인해 유발되는 이러한 위험·위협은 경찰활동의 전략에 있어서도 그 심각성에 대한 인식 및 대응의 수위를 높여야 할 것으로 판단된다. 이는 악성코드의 특성 상 불특정 다수 또는 SNS 상에서의 '친구'들과 같은 지인·동료에게 광범위하게 확산, 전파됨으로써 그 피해의 강도나 사회·경제적 측면에서의 폐해도 우려할만한 수준이므로 경찰활동의 전략에 중요한 요소로 반영되어야 하겠다.

SNS 사용자의 프라이버시 침해 문제는 전 세계적으로 주요한 이슈(Issue)로 부각된 위험요소이기도 하다. 가장 핵심적 문제는 SNS 상에서 사용자 프로파일 정보 및 게시자료들을 통한 개인정보의 획득이 용이함과 사용자들에 대한 접촉의 간편성은 범죄자들로 하여금 SNS를 매우 유용한 범죄 실행의 도구로 만들어버린 결과를 낳고 말았다. 더불어 SNS 상에서의 명예훼손과 모욕, 트롤링(Trolling), 집단 따돌림, 스토킹 등 프라이버시 문제와 연계되는 각종 사이버범죄에 악용될 수 있는 소지도 다분하다고 하겠다. 따라서 이러한 부분에 대한 경찰활동의 전략적 접근에 있어서는 현재의 실정법 체계에 대한 보완의 측면과 법제적인 고려가 함께 검토되어야 할 것이다.

한편, 최근 미국과 유럽 등지를 중심으로 가장 심각한 사회적 문제로 대두되고 있는 것이 SNS를 이용하거나 그 사용자들을 대상으로 한 신원 절도(ID Theft) 및 정보 유출이다. 수많은 해커 또는 범죄자들이 방대한 SNS 사용자들을 목표로 신원

절도나 정보 탈취행위를 저지르고 있으며, 심지어 타인의 SNS 계정(신원)을 가장해서 범법행위를 자행하거나 피해 SNS 사용자에게 재정적 손실을 야기하는 등 그 폐해가 심각한 수준에 이르렀다. 또한 스마트폰 등 휴대폰을 통한 SNS 사용자에 대한 공격도 발견되고 있는 상황이다. 이와 관련하여 경찰활동의 전략과 방향 역시 기술적 진보의 수준 및 공격의 특징에 상응하는 대응방안을 모색해야 할 것이며, 특히 신원 절도나 정보 유출의 국제적 특성을 고려하여 국제공조 강화의 중요성도 반영됨이 옳을 것이다.

더욱이 SNS가 테러집단이나 중범죄자들에 의해서도 악용되고 있는 실정을 감안할 때 인터폴(Interpol)을 통한 국제협력뿐만 아니라 각 국가 간 법제의 차이로 인한 난관을 줄이고 수사의 효과성 거양을 위한 다자간(Multi-lateral) 또는 양자간(Bi-lateral) 협약이나 신종 사이버·디지털 범죄 관련 국제협정(Convention) 체결의 필요성도 장기적으로 검토해야 할 것이다. 지난 2010년 인터폴 사무총장의 페이스북 계정 신원 절도 사건이나 페이스북을 통한 아동 포르노 확산 사례, 그리고 SNS 상에서 스테가노그래피 기법을 이용한 테리리스트들의 은닉 통신 등을 고려할 때 장기적이고도 예방적인 경찰활동 전략의 수립과 이행은 매우 시의적절하고도 중요한 의미를 가진다 하겠다.

마지막으로 SNS와 수사·사법기관의 도·감청 문제와 관련하여 미국의 경우를 사례로 제시하였으나, 현재의 한국 사회 및 법체계 하에서 미국 사례의 수평적 전이를 통한 반영은 그다지 현실성 있거나 혹은 바람직하지 않아 보일 수 있을 것이다. 다만 미국의 경우 국익 보호, 국가안보 수호, 테러 예방 및 대응이라는 거시 목표 하에서는 법제적 고려를 통해 SNS 통신 영역과 그 내용에 대한 수사·사법·정보기관의 도·감청을 보장해 두고자 하는 시도를 엿볼 수 있었다. 비록 국내 실정과 맞지 않거나 혹은 현행 법체계에 대한 직접적 반영·고려 여부는 별개의 문제로 차치하더라도, SNS가 내포하는 위험 및 위협에 대한 심각성의 인식과 국가적·사회적 차원에서의 적극적 대응의 필요성에 관한 부분은 국내 경찰활동 전략 수립과 대응방안 모색 측면에서 충분히 그 의미와 가치가 있는 비교·검토의 사안이라고 할 것이다.

이상과 같이 이 연구에서는 SNS의 위험성 및 위협, 그리고 그것이 Policing (경찰활동)에 미칠 수 있는 영향에 관해 살펴보고자 탐색적 시도를 하였다. 다만 이 연구는 SNS의 위험성과 위협 및 경찰활동에 미치는 영향을 고찰하기 위해 유사 선행연구 사례 및 문헌자료를 중심으로 시론적인 연구를 진행하였지만 실제로 SNS가 내재

하고 있거나 유발하는 각각의 위험·위협요소가 경찰의 범죄예방이나 치안질서 유지 활동에 어떻게 직·간접적 영향을 미치는지 또는 연관성의 정도가 어떠한지를 검증해보지는 못한 한계가 있다고 하겠다. 따라서 후속 연구에서는 범죄수사 또는 경찰자원(Police Resources)의 효과적 활용 등의 경찰활동에 SNS가 미치는 영향에 대하여 보다 심도 있는 연구가 진행될 수 있기를 기대한다.

참고문헌

1. 국내문헌

경찰청 (2010). 경찰백서.

김중태 (2010). 소셜네트워크가 만드는 비즈니스 미래지도: 세계를 강타하는 네트워크 미래혁명. 서울: 한스미디어.

김지용, 손동환, 김현진 (20100). 소셜 네트워크 서비스 기술 동향. 전자통신동향분석 26(3), 14-24.

매튜 프레이저·수미트라 두타, 최경은 역 (2010). 소셜 네트워크 e-혁명. 서울: 행간.

민병원 (2006). 네트워크 시대의 위험과 국가안보 개념의 재정립. 안보학술논집 17(1), 1-73.

이왕휘 (2008). 울리히 벡의 세계위험사회. 한국위기관리논집 4(1), 63-71.

이재열 (2004). 위험사회와 생태적 · 사회적 안전. 서울: 정보통신정책연구원.

이재열 (2005). 사회안전지표 개발을 위한 국민 안전의식 조사. 서울: 소방방재청.

이재열, 안정옥, 송호근 (2007). 네트워크 사회의 구조와 쟁점: 관계와 상징의 연결망(III). 서울: 서울대학교출판부.

이형효 외 (2009). SNS 환경의 아이덴티티 공유 및 보호에 관한 연구. 정보보호학회논문지 19(1), 103-114.

최봉, 변미리 (2011). 소셜 네트워크 서비스와 서울시 활용방안 연구. 서울: 서울시정개발연구원.

최진혁 (2010). SNS가 산업보안적 측면에서 가지는 위험성. 한국산업보안연구학회 2010년 정기 학술세미나.

카스텔, M., 박행웅 역 (2004). 인터넷 갤럭시. 서울: 한울아카데미.

하지철, 이동한 (2010). 마케팅조사 실무노트 III. 서울: 이담북스.

2. 해외문헌

Abdel-Aziz, Ahmed (2008). *Espionage - Utilizing Web 2.0, SSH Tunneling and a Trusted Insider,* Bethesda, MD: SANS Institute.

Beck, Ulrich (1992). *Risk Society: Towards a New Modernity*, [Translated from Risiko- gesellschaft: Auf dem Weg in eine andere Moderne (1986)], New Delhi: Sage.

Borodzicz, E. P., Risk (2005). *Crisis and Security Management*, West Sussex, England: John Wiley

& Sons, Inc.

Breaux, Travis and Anton, Annie (2008). Analyzing Regulatory Rules for Privacy and Security Requirements. *IEEE Transactions on Software Engineering 34(1)*, 5-20.

Bureau of Justice Statistics (2007). *Identity Theft 2005 (National Crime Victimization Survey)*, Office of Justice Programs, U.S. Department of Justice.

Cappelli, Dawn M. & Moore, Andrew P. (2008). Risk Mitigation Strategies: Lesson Learned from Actual Insider Attacks (Session Code: DEF-203, RSA Conference 2008). *CERT Program - Software Engineering Institute*, Carnegie Mellon University.

Cartrysse, Kathy, et al. (2004). *Using licenses and private computing as PET(Privacy- Enhancing Technologies).* The Netherlands: Privacy in an Ambient World (PAW).

Castells, Manuel (2003). *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford: Oxford University Press.

Caudle, Rodney (2009). *Investigative Tree Models,* Bethesda, MD: SANS Institute.

Cisco Whitepapers (2008a). *Data Leakage Worldwide: Common Risks & Mistakes Employees Make*, San Jose, CA: Cisco Systems, Inc.

Cisco Whitepapers (2008b). *Data Leakage Worldwide: The High Cost of Insider Threats,* San Jose, CA: Cisco Systems, Inc.

Computer Security Institute(CSI) (2009). *CSI Computer Crime and Security Survey*, NY: CSI.

Copes, Heith & Vieraitis, Lynne (2007). *Identity Theft: Assessing Offenders' Strategies and Perception of Risk,* U.S. Department of Justice.

Dinerman, Brad (2011). *Social Networking and Security Risks,* GFI White Paper, Gary, NC: GFI.

Ericson, R. V. and Haggerty, K. (1997). *Policing the Risk Society,* University of Toronto Press.

Ernst & Young (2009). *Outpacing Change: Ernst & Young's 12th Annual Global Information Security Survey*, Ernst & Young.

Filkins, Barbara & Radcliff, Deb (2008). *Data Leakage Landscape: Where Data Leaks and How Next Generation Tools Apply*, Bethesda, MD: SANS Institute.

Fisher, Tony (2009). *The Data Asset: How Smart Companies Govern Their Data for Business Success,* Hoboken, NJ: John Wiley & Sons, Inc.

Fowler, J. H., Dawes, C. T., and Christakis, N. A. (2009). Model of Genetic Variation in Human Social Networks. *Proceedings of the National Academy of Sciences 106(6),* 1720-1724.

Gaines, Larry K. & Cordner, Gary W. (eds.) (1999). *Police Perspective: An Anthology*, Roxbury.

Garcia, Joseph (2009). *Mitigating Insider Sabotage*, Bethesda, MD: SANS Institute.

Girard, John and Wagner, Ray. (2007). *Magic Quadrant for Mobile Data Protection,* Research Note G00151075, Stamford, CT: Gartner, Inc.

He, Qingfeng and Anton, Annie I. (2009). Requirements-based Access Control Analysis and Policy Specification (ReCAPS). *Information and Software Technology* 51(6), 993-1009.

Identity Theft Resource Center(ITRC) (2010). *2009 Data Breach Stats, Office for Victims of Crime*, Office of Justice Programs, U.S. Department of Justice.

Identity Theft Resource Center(ITRC) (2010). *2009 ITRC Breach Report, Office for Victims of Crime,* Office of Justice Programs, U.S. Department of Justice.

Identity Theft Resource Center(ITRC) (2010). High Profile Breach Report, ITRC.

Jarvis, Darryl S. L. (2010). *Theorizing Risk: Ulrich Beck, Globalization and the Rise of the Risk Society,* National University of Singapore.

Johnston, L. & Shearing, C. D. (2003). *Governing Security: Explorations in Policing and Justice,* New York: Routledge.

Kendricks, Walter (2008). *A Guide to Mitigating the Insider Threat,* Presented at the Information Security Officer Meeting, Hosted by California Office of Information Security and Privacy Protection.

Kim, D. S., Jung, Y. J., and Chung, T. M. (2005). PRISM: A Preventive and Risk-Reducing Integrated Security Management Model Using Security Label, *The Journal of Super-computing* 33(1), 103-121.

Lovelock, C., Patterson, P. G., and Walker, R. H. (1998). *Services Marketing,* Sydney: Prentice-Hall.

Morgan Stanley (2009). *Economy & Internet Trends*, Morgan Stanley.

Newman, Graeme R. (2004). *Identity Theft,* U.S. Department of Justice.

Office of Information Security and Privacy Protection (2008). The Hostile Takeover, *Insider Threats*, Information Sheet No. 5.

Ouellet, Eric and Proctor, Paul E. (2008). *Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention,* Gartner RAS Core Research Note G00157450, Stamford, CT: Gartner, Inc.

Purpura, Philip P. (2007). *Terrorism and Homeland Security: An Introduction with Applications*, Burlington, MA: Butterworth-Heinemann.

Raschke, Thomas (2008). *The Forrester Wave: Data Leak Prevention,* Q2 2008, Cambridge, MA: Forrester Research, Inc.

Rubenstein, H., et al. (1980). *The Link Between Crime and The Built Environment,* Washington, D.C.: National Institute of Justice.

Taylor-Gooby, P. & Zinn, Jens O. (2006). Risk in Social Science, Oxford: Oxford University Press.

Tucker, D. (2001). What's New About the New Terrorism and How Dangerous Is It?, *Terrorism*

and Political Violence 13, 1-14.

U.S. Secret Service & Carnegie Mellon University's Software Engineering Institute (CERT) (2008). *Insider Threat Study: Illicit Cyber Activity in the Government Sector,* U.S. Department of Homeland Security.

Van Blarkom, G. W., Borking, J. J. and Olk, J. G. E. (eds.) (2003). *Handbook of Privacy and PET(Privacy-Enhancing Technologies)*, The Hague, The Netherlands: PISA Consortium / College Bescherming Persoonsgegevens.

Verizon Business RISK Team (2008). *2008 Data Breach Investigations Report*, Basking Ridge, NJ: Verizon Business.

Wasserman, Stanley and Faust, Katherine (1994). *Social Network Analysis: Methods and Applications*, Cambridge: Cambridge University Press.

Weisman, Robyn (2010). Preventing Data Leaks: A Dose Of Security Savvy Will Help Plug The Cracks In Your Data Center, *Processor* 32(2), 32.

Wellman, Barry (2001). Physical Place and Cyber Place, *International Journal of Urban and Regional Research.*

Wellman, Barry, et al. (2003). The Social Affordances of the Internet for Networked Individualism, *Journal of Computer-Mediated Communication 8(3).*

Utz, S., & Kramer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms, *Cyberpsychology: Journal of Psychosocial Research on Cyberspace 3(2)*, article 1.

3. 인터넷 자료

디지털타임스(Digital Times), "전 세계 2억 8000만 명 개인정보 유출됐다: KISA, 지난 3년간 부주의·해킹으로," http://www.dt.co.kr/contents.html?article_no=2008111202010351713002, 2008.

보안뉴스, "유비쿼터스 사회의 개인정보 보호에 관한 연구," http://www.boannews.com/media/view.asp?idx=10432&kind=1#, 2008.

보안뉴스, "디지털 시대, 개인정보보호 실태와 대응법," http://www.boannews.com/media/view.asp?idx=18308&kind=4&search=title&find=%B5%F0%C1%F6%C5%D0%BD%C3%B4%EB+%B0%B3%C0%CE%C1%A4%BA%B8%BA%B8%C8%A3, 2009.

보안뉴스, "정보보안 투자 없는 기업, 성공신화도 없다," 월간 정보보호21C (제113호), http://www.boannews.com/media/view.asp?idx=19166&kind=1#, 2010.

세계일보(2010), "소셜 네트워크 서비스(SNS) 전성시대," http://www.segye.com/Articles/FAMILYGLOBAL/ECOLUMN/Article.asp?aid=20100525000660&cid=010601090000

0&subctg1=09&subctg2=00, 2010.

아시아경제, "개인금융정보 50만 건 '해킹'에 범죄조직 개입," http://www.asiae.co.kr/news/view.htm?idxno=2008110116025733602, 2008.

안철수연구소(AhnLab), "2010년 이슈가 될 보안 위협 12가지", http://ahnlabgirl.cafe24.com/ahnlab/765, 2010.

전자신문, "'개인정보 침해를 막자' 美, 관련법안 속속 통과," http://www.etnews.co.kr/news/detail.html?id=200911060082, 2009.

BBC News, "Trojan virus steals banking info," http://news.bbc.co.uk/2/hi/7701227.stm, 2008.

BusinessWeek, "Countries with the Most Cybercrime," http://images.businessweek.com/ss/09/07/0707_ceo_guide_security/index.htm, 2009.

Child Sexual Abuse, Medline Plus, U.S. National Library of Medicine [http://www. nlm.nih.gov/medlineplus/childsexualabuse.html], 2011.

Collins, Brendan, "Privacy and Security Issues in Social Networking", http://www.fastcompany.com, 2008.

Compuware Corporation, "Compuware Study Shows Insiders Pose Biggest Threat to Data Security: Employing Best Practices and Technology Can Protect Sensitive Data, Maintain Company Reputation and Prevent Financial Losses," http://investor.compuware.com/releasedetail.cfm?ReleaseID=340003, 2008.

Daily Mail, Computer Weekly, and Yonhap News, "인터폴 총장 "페이스북서 신원 도용 당해"," http://www.computerweekly.com/news/1280093823/Interpol-chief-admits-Facebook-ID-theft, 2010.

George, Allison, "Living online: The end of privacy?," *New Scientist*, 2569, http://www.newscientist.com/channel/tech/mg19125691.700-living-online-the-end-of-privacy.html, 2006.

Goodin, Dan, "Data collector charged $275,000 for leaking personal data: $20 a head. 13,750 heads," The Register, http://www.theregister.co.uk/2009/10/20/ftc_fraud_ crackdown, 2009.

Greenberg, Andy, "Plugging The Government's Biggest Data Leak," Forbes, http://www.forbes.com/2009/12/15/cybersecurity-government-ferriero-technology-cio-network-nara.html, 2009.

Identity Theft Resource Center(ITRC), "Security Breaches 2008," http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml, 2009.

Identity Theft Resource Center(ITRC), "Data Breaches: The Insanity Continues," http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2009.shtml, 2010.

IT Daily, "개인정보 유출사고의 원인과 정책 방향 (박 광진)," http://www.itdaily.kr/news

/articleView.html?idxno=16189, 2008.

IT Daily, "'개인정보 유출 등 보안사고'가 기업 이미지에 가장 나쁜 영향 준다," http://www.itdaily.kr/news/articleView.html?idxno=19336, 2009.

McAfee, "Social Networking Apps Pose Surprising Security Challenges," http://www.mcafee.com/, 2010.

Office of the Privacy Commissioner for Personal Data, Hong Kong, "Privacy Commissioner investigates Police data leakage incident," http://www.pcpd.org.hk/english/infocentre/press_20090309.html, 2009.

Symantec, "Symantec Internet Security Threat Report Tracks Notable Rise in Cyber -crime Activity," http://www.symantec.com/about/news/release/article.jsp?prid=200603 07_01, 2006.

The Day, "State sues Health Net over data leak," http://m.theday.com/theday/db_39913/contentdetail.htm;jsessionid=A1EE656405A0404493474004EF562A4D?contentguid=iaLdRa4h&detailindex=1&pn=0&ps=3&full=true, 2010.

The Register, "Hackers pluck 8,300 customer logins from bank server," http://www.theregister.co.uk/2010/01/12/bank_server_breached, 2010.

Young, Tom, "Data losses hit 280 million people," Computing, http://www.v3.co.uk/computing/news/2230048/losses-hit-280-million-kpmg, 2008.

인터넷 통계정보 검색시스템(ISIS). https://isis.nida.or.kr/

한국인터넷진흥원(KISA). http://www.kisa.or.kr/

한국정보화진흥원(NIA). http://www.nia.or.kr/

Bureau of Justice Statistics. http://bjs.ojp.usdoj.gov/

California Office of Information Security. http://www.cio.ca.gov/OIS/

California Office of Privacy Protection. http://www.privacy.ca.gov/

Identity Theft Resource Center®(ITRC). http://www.idtheftcenter.org/

National Criminal Justice Reference Service. http://www.ncjrs.gov/

Privacy Rights Clearinghouse. http://www.privacyrights.org/

The New York Times. http://www.nytimes.com/

The Washington Post. http://www.washingtonpost.com/

【Abstract】

An Exploratory Study on the Risks and Threats of SNS(Social Network Service): From a Policing Perspective

Choi, Jin-Hyuk

This exploratory study aims to review the risks and threats of social network services(SNSs), particularly focusing upon the policing perspective. This paper seeks to acknowledge the present risk/danger of SNSs and the very significance of establishing a strategic framework to effectively prevent and/or control criminal misuse of SNSs. This research thus advocates that proactive study on security issues and criminal aspects of SNSs and preventive countermeasures can play a significant role in policing the networked society in the time of digital/internet age.

Social network sites have been increasingly attracting the attention of entrepreneurs, and academic researchers as well. In this exploratory article, the researcher tried to define concepts and features of SNSs and describe a variety of issues and threats posed by SNSs. After summarizing existing security risks, the researcher also investigated both the potential threats to privacy associated with SNSs, such as ID theft and fraud, and the very danger of SNSs in case of being utilized by terrorists and/or criminals, including cyber-criminals.

In this study, the researcher primarily used literature reviews and empirical methods. The researcher thus conducted extensive case studies and literature reviews on SNSs. The literature reviews herein cover theoretical discussions on characteristics, usefulness, and/or potential danger/harm of SNSs. Through the literature review, the researcher also concentrated upon being able to identify a strategic framework for law enforcement to effectively prevent

criminal misuse of SNSs

The limitation of this study can be lack of statistical data and attempts to examine previously un-researched area in the field of SNS and its security risks and potential criminal misuse. Thus, to supplement this exploratory study, more objective theoretical models and/or statistical approaches would be needed to provide law enforcement with sustainable policing framework and contribute to suggesting policy implications.

Key Words : SNS(Social Network Service), Risks, Threats, Policing, Security, Cyber-crime, Privacy