

NIA

2012년 하반기 개인정보보호 해외 정책 동향

개인정보보호기획부 / 2012. 12.

>>> 목 차

이슈

아시아 주요국의 최근 개인정보보호 정책 동향

1

개인정보보호 제도의 정비와 집행기구의 권한 확대

유럽평의회, Convention 108 개정안 작업 박차	10
美 캘리포니아주, 프라이버시 감독 및 모니터링 기구 설치	12
美 연방정부 계약자의 데이터 보호 규정 마련	14
EU 집행위, 데이터 보호 규정 개편 의견서 발표	16
EU, 중소기업에 대한 데이터보호 규정 완화 준비	17
EU, DPO(Data Protection Officer) 에 관한 조사 보고서 발간	18
호주, Privacy Act 수정안 의결, 감독기구 권한 확대	19

2

빅데이터와 클라우드 환경에서의 개인정보보호 기반 강화

EU 집행위원회, 클라우드 환경에서의 프라이버시 보호 추진방향 제시	22
아일랜드 데이터보호 감독원, 클라우드 보안 가이드 발행	24
이탈리아, 클라우드 서비스 이용에 따른 개인정보보호 10대 수칙 발표 ..	26
CSA-후지츠, 빅데이터 작업 그룹 공동 설립	27
ICDPPC, 빅데이터 시대에서의 개인정보 프로파일링 선언문 발표	28
영국 ICO, 데이터 익명화 실행규칙 제정	30

3 모바일환경 보편화와 위치정보·스마트폰 관련 조치 확대

프라이버시 미래 포럼, 모바일 앱 조사 연구 결과 발표	33
美 이통사, FCC 프라이버시 강화 반대 입장 표명	35
美 캘리포니아주 의회, 위치 프라이버시 법안 통과	37
美 FTC, 앱 개발자들을 위한 가이드 제공	39
캐나다 프라이버시 위원회, 앱 개발 가이드라인 제시	40
ACT, 앱 프라이버시 아이콘 개발 보급	42
美 FCC, 스마트폰 이용자를 위한 보안 가이드 발표	43

4 얼굴인식기술의 발달과 영상정보처리기기의 규제 강화

영국 ICO, 사우샘프턴 의회에 차량 내 음성녹음 금지 명령	46
페이스북의 Photo Tag Suggest 기능에 대한 제재 움직임 확산	47
위키리크스, 미국 정부의 대테러 소프트웨어 사용 폭로	48
美, 무인 항공기에 대한 프라이버시 보호 법안 제안	49
美 FBI, 차세대 얼굴 인식 시스템 도입	51
美 FTC, 프라이버시 관련 얼굴인식기술 사용 가이드라인 제시	53

5 글로벌 협력 인식 및 제도간 상호운용성 노력 확대

EU, Data Processor 용 BCR(Binding Corporate Rule) 개발	55
캐나다 - 독일, 데이터 보호 감독기구간 상호 협력 체결	57
국가별 EU 개인정보보호 Adequacy 평가 진행 경과	58

6

엔터테인먼트 분야와 어린이 개인정보보호 관심 증가

블리자드 Battle.net, 중국을 제외한 모든 이용자 정보 유출	62
영국 ICO, 학교 대상 정보보호 가이드 발행	63
캐나다, 프라이버시 관련 비디오게임 가이드라인 제시	65
美 FTC, 어린이용 앱 프라이버시 실태조사 실시	66
美 FTC, 어린이 온라인 프라이버시 보호법 개정	67

7

기타

영국 ICO, 공공분야 직원의 개인정보 사용에 대한 안내서 발간	69
캐나다 IPC, Privacy by Design 안내서 발간	70
OCR, 의료 개인정보 관련 익명화 가이드 발표	71

[부록] 인터넷 세상의 두 빅브라더 : 구글과 페이스북의 개인정보보호 이슈

이슈 : 아시아 주요국의 최근 개인정보보호 정책 동향

- 지난 몇 개월 동안 아시아 지역 개인정보보호 정책에 큰 변화가 있었음
 - ▶ 필리핀과 싱가폴은 최초로 데이터 프라이버시 법을 제정,
말레이시아는 몇 년간 수정후 포괄적인 데이터 프라이버시 법안 시행 예정,
호주·홍콩·대만은 현행 개인정보보호 법안을 개정
 - ▶ 대부분의 아시아 국가가 개인정보 처리를 위한 제한된 조건이나 법적조건을 마련하는 EU와 같은 접근법을 사용하나 최근 국가별 환경과 상황에 맞게 개인정보보호법안을 제정하거나 개정하는 방향으로 나아가고 있음

1. 신규 프라이버시 법안 제정 국가

□ 말레이시아

- (경과) 2009년 정부에 제안되었던 "Personal Data Protection Act"가 2010년 의회에서 승인, 2013년 1월부터 법적 효력 발효 예정
- (적용범위) 말레이시아 내에서 처리되거나, 국외에서 처리되었지만 말레이시아 내에서 추가적인 처리가 필요한 모든 개인 정보가 적용 대상
- (골자) 말레이시아의 "Personal Data Protection Act"의 주요 내용
 - 고지 및 동의 : 데이터처리자는 개인정보 수집과 처리에 대해 공지해야 하고 개인정보처리를 위해서는 정보주체 동의 필요
 - 보안 및 유지 : 개인정보를 분실, 오용, 조작, 비인가된 접근, 유출, 수정, 폐기로부터 보호하기 위해 적절한 보호 절차를 마련해야 하고 불필요한 장기 데이터 보관 금지
 - 접근 및 수정권 : 정보주체에게 자신의 정보에 대해 열람하고 수정할 수 있는 권한 부여
 - 국외이전 : 개인정보 국외 이전을 위해서는 정보통신문화부 장관의 승인 필요 (사전 동의, 계약 요건 등 예외사항 별도 규정)

- 독립된 총괄기구 설립 : 개인정보보호위원회(Personal Data Protection Commissioner) 설립, 법 준수 여부 감독, 조사(inspection), 모니터링 및 관계부처 집행 관련 자문 수행
- 개인정보처리 등록 : 조직 유형에 따라 개인정보처리에 대한 등록 의무화, 공공분야 기관은 개인정보처리에 대한 자격을 획득해야만 관련 업무 가능
- 처벌규정 : "Personal Data Protection Act" 위반 시, 형사처리 및 벌금 집행 실시, 최고 USD 164,000의 벌금 그리고/혹은 2년의 징역을 선고

□ 필리핀

- (경과) 2012년 9월 "Data Privacy Act of 2012 (the Philippine Act)"가 발효되어 법집행을 시작하였으며 90일 내에 세부 규제 마련 예정
- (적용범위) 공공기관 및 민간 기업에서 다루는 모든 개인 정보가 적용 대상
 - ※ 예외사항 : 재외국적 거주자 정보, 자금세탁방지법에 의거하여 요구되는 개인정보, 공공 업무 수행을 위해 필요한 정보 등은 예외로 둠
- (골자) "Data Privacy Act of 2012 (the Philippine Act)"의 내용은 다음과 같음
 - 총괄기구 설치 : 정보통신기술부 산하에 국가 프라이버시 위원회 설치
 - 데이터 보호 관리자(Data Protection Officer, DPO) : 모든 데이터 처리자는 반드시 한명 이상의 DPO를 임명토록 함
 - ※ 데이터베이스 등록은 공공은 의무사항, 민간은 자율적으로 추진
 - 고지 및 동의 : 개인정보 수집 및 처리를 위해 개인정보 수집, 처리, 공유, 개인정보 접근 권한, 개인정보관리 책임자 연락처 정보를 제공하고 제 3자에게 개인정보 처리 및 제공할 때 동의 필요
 - 보안 및 유지 : 합리적이고 적절한 조직적, 물리적, 기술적 보호 조치 마련 필요
 - 접근 및 수정권 : 개인에게 반드시 개인정보에 접근하여 수정하고 변경할 수 있는 권한 부여
 - 국외이전 : 국내에서의 이전 조건과 동일하게 적용
 - 유출통지 : 민감정보와 관련하여 위법사항 발생시, 즉시 국가 프라이버시 위원회와 피해자에게 관련 내용 통지

- 처벌규정 : "Data Privacy Act of 2012 (the Philippine Act)" 위반 시, 최소 6개월에서 최고 6년의 징역과 USD 12,000에서 USD 120,000의 벌금 선고

□ 싱가포르

- (경과) 싱가포르 입법부는 2012년 10월 "Personal Data Protection Act 2012"를 승인, 2013년 1월부터 법적 효력 발생
- (적용범위) 싱가포르에 위치한 모든 민간 기업이 적용대상
 - ※ 다른 기업을 대신하여 처리하는 서비스를 제공하는 경우는 제외
- (골자) "Personal Data Protection Act 2012 (PDPA)" 주요 내용
 - 총괄기구 설치 : 개인정보보호위원회를 설립하고, 감독·집행·처벌 권한 부여
 - DPO 지정 : 모든 기업은 최소 한 명의 데이터 보호 관리자를 두어 PDPA 준수여부 확인
 - 고지 및 동의 : 데이터 운영자는 데이터 주체에게 개인 데이터 수집, 사용, 제공 목적을 밝히고 동의 요청
 - 보안 및 유지 : 기업이 개인정보보호를 위해 갖추어야 할 일반적인 의무사항을 명시하고 데이터 수집 목적에 따라 더 이상 사용되지 않을 경우 즉시 폐기
 - 접근 및 수정권 : 정보주체 요청시, 기업이 관리·통제하고 있는 개인정보 제공, 정보주체는 본인의 정보 수정과 삭제 요청권리 보유
 - 국외이전 : 일반적으로 PDPA의 요구수준에 상응한 수준인 경우에만 국외 전송이 가능
 - ※ 현재 국외이전과 관련하여 PDPA의 상세한 규정과 범위가 정해지지 않음
 - 처벌사항 : PDPA 위반 시, 최고 USD 8,000의 벌금과 3년 이하의 징역이 선고, 개인정보보호위원회에 최고 USD 800,000의 벌금을 부과권한 부여

2. 현행법의 개정 국가

□ 호주

- (경과) The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 가 2012년 11월 29일 의회에서 통과됨
- (개정 내용) 개정된 법안 내용은 다음과 같음
 - Privacy Act 1988을 Australian Privacy Principle (APPs)로 수정하여 공공 기관 및 민간 기업에 통일된 프라이버시 원칙 제공
 - APPs와 신용평가보고 법규에 따른 실행규칙을 제공하는 포괄적인 신용 평가보고시스템 적용
 - 프라이버시 보호 위원회 권한 강화

□ 홍콩

- (경과) 2012년 7월, "The Personal Data (Privacy) (Amendment) Ordinance 2012" 채택, 대부분의 개정 내용이 2012년 10월에 발효되었으나 다이렉트 마케팅 부분은 2013년 상반기 발효
- (개정 내용) 다이렉트 마케팅에서의 개인정보 사용에 대해 보다 상세히 규제, 데이터 보호 원칙과 벌금 그리고 개인 데이터 프라이버시 위원회 권한 강화

□ 대만

- (경과) "1995 Computer Processed Personal Data Protection Act"가 "Personal Data Protection Act and Enforcement Rules" 으로 개정, 2012년 10월부터 발효
- (개정 내용) 개인정보범위가 모든 공공 기관 및 민간 기업 그리고 모든 업종으로 확대, 개인의 의료관련 정보보호 내용 포함, 개인정보사용을 원하는 정보 수집자는 개정법안 발효 후 일년내 정보주체로부터 동의 필요

[자료출처]

<http://www.globallawwatch.com/products/privacy/privacy-security-law-report/>

1 개인정보보호 제도의 정비와 집행기구의 권한 확대

- ▷ 유럽평의회, Convention 108 개정안 작업 박차
- ▷ 美 캘리포니아州, 프라이버시 감독 및 모니터링 기구 설치
- ▷ 美 연방정부 계약자의 데이터 보호 규정 마련
- ▷ EU 집행위, 데이터 보호 규정 개편 의견서 발표
- ▷ EU, 중소기업에 대한 데이터보호 규정 완화 준비
- ▷ EU, DPO(Data Protection Officer) 에 관한 조사 보고서 발간
- ▷ 호주, Privacy Act 수정안 의결, 감독기구 권한 확대

유럽평의회(CoE), Convention 108 개정안 작업 박차

요 약

- 유럽평의회(Council of Europe, CoE)는 지난 2010년부터 시작된 Convention 108의 개정작업에 박차를 가하고 있으며 내년까지 완료 예정
- (배경) 2010년 3월, 유럽평의회 (Council of Europe)가 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (이후 Convention 108)의 개정작업을 시작
 - 1981년에 제정된 Convention 108은 유럽의 데이터 보호법에 큰 영향을 끼친 법으로써, 데이터 보호 지침 1995(Directive 95)의 근간이 되었음
 - (개요) 2012년, 유럽평의회는 2011년에 있었던 공개자문 및 유럽 각국의 제안을 바탕으로 Convention 108의 개정안 작업 실시
 - 정보통신 기술의 변화에 따른 프라이버시 보호의 변화에 대응 요구
 - (내용) 개정목표 및 주요 이슈
 - 새로운 정보통신기술의 사용과 더불어 프라이버시의 변화에 대응
 - Convention108의 후속조치 메커니즘을 강화
 - Convention108의 원칙은 지속하되 더 구체적인 권고안과 가이드라인으로 보완
 - EU의 법적 프레임워크와의 일관성과 상호운용성, 기술적 중립성 확립
 - 전 세계적인 표준으로써의 Convention108의 잠재성 재확립
 - 개정의 주요 이슈
 - (데이터와 관련된) 과잉금지, 데이터 최소화
 - 책임성
 - Privacy by Design

- 데이터 유출 신고 의무
 - 데이터 처리의 투명성
 - 데이터 주체를 위한 안전장치 (데이터 소스 접근 권리, 데이터 처리에 관한 정보를 얻을 권리, 거부할 권리 등)
- **(향후 방향)** 2012년과 2013년, Convention 108의 개정에 업무의 우선 순위를 두어 개정작업에 박차를 가할 예정

[자료출처]

<http://fra.europa.eu/fraWebsite/symposium2012/docs/council-of-europe-convention-108-Polakiewicz.pdf>

http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

美 캘리포니아州, 프라이버시 감독 및 모니터링 기구 설치

요 약

- 모바일 플랫폼 운영사와의 합의서의 내용을 바탕으로 캘리포니아주는 사법부 내 프라이버시 감독 및 모니터링 기구인 Privacy Enforcement and Protection Unit 설치
- 해당 기구를 통해 합의서 내용 준수 여부 모니터링과 프라이버시 관련 법집행, 교육, 기업과의 파트너십 도모 등의 기능을 수행할 것임

※ 합의서 내용은 불임 참조

○ **(배경)** 2012년 초 구글이 사파리 보안설정을 우회하여 사용자의 웹 사용을 추적해 온 사건과 작년 애플 모바일 기기 내 위치정보수집과 같이 프라이버시 이슈 발생으로 프라이버시에 대한 우려 확대

※ 2012년 6월 Future of Privacy Forum에 따르면 iTunes App Store, Google Play, Amazon Appstore 내 top-selling 150개의 앱 중 평균 61.3%가 프라이버시 정책 보유

- 이에, 정보화시대의 프라이버시 이슈에 대응하기 위해 캘리포니아주는 프라이버시 감독 및 모니터링 기구인 Privacy Enforcement and Protection Unit 설립

○ **(구성 및 기능)** 2012년 2월 모바일 플랫폼 회사들과의 합의서를 근거로 설립된 기구로서 6명의 검사원으로 구성되며 프라이버시 관련 업무를 담당

- 해당 기구는 사법부 내 eCrime Unit의 한 부분으로 속하고 프라이버시 집행과 관련된 6명의 검사원으로 구성

- 담당 기능 : (1) 프라이버시 관련 법집행, (2) 프라이버시 교육, (3) 프라이버시 증진에 대해 회사와의 파트너십 도모, (4) 개인 및 기업의 프라이버시 운영을 감시

○ **(기대효과)** Privacy Enforcement and Protection Unit의 설립으로 캘리포니아주는 연방거래위원회 (FTC, Federal Trade Commission)보다 보다 신속하게 프라이버시 이슈 처리 기대

[붙임 : 합의서 주요 내용]

- o 2012년 2월, 캘리포니아 주는 Apple, Google, RIM, Amazon, HP, MS와 같은 모바일 플랫폼 회사와 다음과 같은 프라이버시 보호 내용에 합의함
- (1) 캘리포니아 온라인 프라이버시 보호 법안에 따라 프라이버시 보호 정책을 준비
 - (2) 사용자가 앱을 다운로드하고 설치하기 전에 모바일 앱에 대한 프라이버시 정책을 검토하게끔 함
 - (3) 플랫폼 회사는 앱 개발자 대상으로 고객의 프라이버시를 존중하고 정보 수집, 사용, 공유에 대한 내용을 고객에게 공개하게끔 교육 실시
 - (4) 합의 내용을 미준수하는 앱 발견 시, 고객이 제보할 수 있는 톨을 마련하고 회사는 이에 대응하는 절차 준비
 - (5) 6개월 내 합의 내용과 관련한 프라이버시 평가를 실시

[자료출처]

http://www.computerworld.com/s/article/9229383/California_to_get_tough_on_online_privacy

<http://www.informationweek.com/news/government/policy/240004137>

<http://www.infoworld.com/d/security/mobile-app-stores-require-disclose-privacy-policies-187109>

<https://www.privacyrights.org/ar/CAPrivProtAct.htm>

<http://esininja.com/blog/2012/07/20/california-ag-creates-privacy-enforcement-and-protection-unit/>

<http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>

美 연방 정부 계약자의 데이터 보호 규정 마련

요 약

- 미국은 USD 10만 이상의 상용물자와 소규모 비즈니스 대상 연방 계약자에게 기본적인 데이터 보호 정책을 마련할 것을 요구
- 규정 채택 시, 계약자의 정보 시스템 상에 있거나 해당 시스템을 거쳐 가는 비공개 정보에 대한 유출 방지 기대

- **(배경)** 현재 Federal Acquisition Regulation (FAR)이 정부에 의해 제공되거나 정부를 위해 처리되는 데이터에 대한 보호 규정이 미비로 인해 보완이 불가피
- **(내용)** ‘Basic Safeguarding of Contractor Information Systems’에서 다음 내용을 요건으로 포함
 - 접근통제가 미비한 공공 컴퓨터를 이용하여 정부의 비공개 정보처리를 금함
 - 이메일, 문자 메시지, 블로그 등을 통해 정부의 비공개 정보를 전송 시, 최고 수준의 보안과 프라이버시 보호를 제공하는 기술을 사용할 것
 - 인가된 수신자에게 정확히 수신된다는 확신이 있을 때에만 정부의 비공개 정보를 음성 또는 팩스로 송부할 것
 - 정부의 비공개 정보 보호를 위해 적절한 논리적·물리적 통제 환경 마련할 것
 - 정부 비공개 정보가 저장된 미디어 파기 시, 적절한 절차에 따라 시행할 것, 예컨대, 오버라이팅을 할 경우, National Institutional of Standards and Technology (NIST)에 명시된 절차를 따를 것
 - 안티 바이러스/스파이웨어를 설치 및 업데이트 하고 정보시스템과 관련된 보안 패치 설치할 것
 - 정부의 비공개 정보는 여기에 규정된 데이터 보호 기준을 따르는 하위 계약자에 한해서 전송 가능함
- **(향후 계획 및 기대효과)** 추가된 신규 규정에 대한 의견을 2012년 10월 23일까지 수렴하며 정부의 비공개 자료의 강화된 보안 수준을 기대

- 이번 규정으로 정부의 비공개 정보에 대한 노출을 최소한으로 하고 비인가자에 접근을 방지할 수 있을 거라 기대
- 이번 규정이 통과되면 정부와 계약을 맺고 있는 모든 회사는 사내 정보시스템과 정보 보안 프로그램에 대해 평가해야 함

[자료출처]

<http://www.gpo.gov/fdsys/pkg/FR-2012-08-24/pdf/2012-20881.pdf>

<http://www.mondaq.com/unitedstates/x/196300/data+protection/Broad+New+Data+Security+Rule+Proposed+For+Federal+Contractors>

유럽집행위, 데이터 보호 규정 개편 의견서 발표

요 약

- 2012년 10월, Article 29 Working Party는 지난 1월 제시된 EU의 일반 데이터 보호 규정(General Data Protection Regulation) 제정과 관련된 두 번째 의견서 발표
- Article 29 Working Party는 EU 데이터 보호법의 프레임워크 개편을 환영하고, '개인 데이터 (personal data)', '동의(consent)', 각국의 위임 사항에 대한 가이드 제시

○ (개요) 2012년 10월, Working Party가 두 번째 의견서를 발표

- Working Party는 의견서에서 EC의 EU 데이터 보호법의 프레임워크 개편을 환영하고, 중요한 개념인 '개인 데이터'와 '동의'에 대한 가이드를 제시, 각국으로의 위임사항에 대한 이슈 제기

※ Article 29 Working Party: EU의 데이터 보존과 관련된 부속 자문기관

○ (주요내용) Working Party의 두 번째 의견서 내용 요약

- 개인 데이터 (Personal Data)에 관한 사항 : data subject(데이터 주체)의 명확한 개념정의 필요
- 개인의 식별성이 개인을 단일하게 지목할 수 있고, 다르게 대할 수 있다는 점을 내포해야 함
- 온라인 식별자 (IP 주소, 쿠키, 위치데이터)는 개인을 식별할 수 있으므로 개인데이터로 규정되어야 함
- 동의(consent)의 정의: 데이터주체가 자신과 관련된 개인데이터의 처리를 동의한다는 것을 명확하게 나타내야 함 (explicit consent)
- 반드시 필요한 사항들만 국가에 위임하고 중요한 규칙의 경우 규정에 포함 할 것을 권고함. 위임할 경우 반드시 구체적인 필요성 및 효과에 대한 평가와 가이드를 제공토록 할 것을 권고

[자료출처]

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf

EU, 중소기업에 대한 데이터보호 규정 완화 준비

요 약

- 유럽 법무 위원회(Europe's Justice Commissioner)는 유럽 연합회 장관들에게 중소기업에게 데이터보호 규정 완화 혜택을 제공을 준비 중이라고 밝힘
- 이번 데이터보호 규정 완화로 법적 환경이 단순화되면 기업은 매년 18억 5천 유로를 절약할 수 있을 거라고 기대

- **(배경)** 유럽 법무 및 안보 협의회 회의에서 Vivian Reding은 중소기업에게 데이터 보호와 관련하여 큰 부담이 되기를 원치 않는다고 성명 발표
- **(내용)** 중소기업은 데이터 보호 관리자를 두지 않아도 되는 예외사항을 이미 적용받고 있으며 법무 위원회는 추가적으로 예외사항 확대를 검토 중이라고 밝힘
 - 처리되는 데이터의 민감도와 양에 따라 데이터 보호 규정의 유연성을 강화하거나 적용 예외 범위 확대를 확대할 것인지에 대해 고려중
- **(향후 방향 및 기대효과)** 법무 위원회는 대형 다국적 기업 이익에 직접적으로 연결된 중소기업에 대해서는 여전히 강력한 데이터 보호 규정을 적용할 것이라고 밝힘
 - 아울러 공공 기관의 경우 일반적인 데이터 정보 보호 규정 예외가 적용되지 않을 것이나 중소기업과 마찬가지로 특별한 경우 데이터 보호 규정의 유연성 강화를 공공기관에 제공할 것이라고 함
 - 이번 데이터 정보 보호 규정 완화가 실행된다면 기업측면에서 매년 18억 5천 유로의 절감효과 기대

[자료출처]

<http://www.computerworlduk.com/news/it-business/3407485/eu-hints-at-data-protection-concessions-for-smes/>

EDPS, Data Protection Officer(DPO)에 관한 보고서 배포**요 약**

- 2012년 12월, 유럽 데이터 보호 감독관(EDPS)이 데이터 보호 담당관(DPO)의 상황에 대한 보고서 배포
- **(배경)** 유럽의 데이터 보호 규정 (EC) No 45/2001의 Article 24에서 각 EU의 기관이나 부서에서 적어도 한명의 데이터 보호 담당관 (Data Protection Officer, 이후 DPO)을 임명할 것을 규정함
 - Article 24에서는 DPO의 임명 조건과 그들의 상태, 업무의 성과에 대한 조건들을 명시함
- 이에, 2012년 12월, 유럽 데이터 보호 감독관 (European Data Protection Supervisor, 이후 EDPS)이 DPO의 상황에 대한 보고서를 배포
- **(내용)** 본 보고서에서 다음과 같이 DPO의 중요 이슈사항을 강조
 - 데이터 보호 지침(Directive 95)의 Article 24에서는 DPO의 임기를 최소 2년이라고 규정하고 있으나, 보고서에 의하면 DPO의 실제 근무기간이 2년보다 짧은 것으로 드러남.
 - DPO가 규정에 의거해 효과적으로 업무를 수행하기 어려운 요인으로서는 DPO 업무와 다른 업무의 병행, 적절한 자원 부족으로 드러남
 - EDPS는 DPO의 독립성과 전문성을 위해 임기를 5년으로 늘릴 것을 권고
- **(향후 기대)** EDPS 보고서에 나타난 문제점을 토대로, DPO 행정인의 경험들을 입법자나 개인정보 저장, 사용 기관들이 고려할 것으로 기대

[자료출처]

<http://www.investineu.com/content/edps-status-dpos-key-safeguarding-data-protection-rights-12c3>

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2012/2012-12-17_DPO_Status_web_EN.pdf

호주, Privacy Act 수정안 의결, 감독기구의 권한 확대

요 약

- 호주 국·내외 프라이버시 위반사건과 IT 기술의 발달에 현재의 Privacy Act가 적절하게 대처하지 못하는 이유로 해당 법안을 수정하기로 결정
- 5월 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012'의 이름으로 2009년 호주 법안 개정 위원회 권고사항이 반영된 수정안이 제출
- 본 개정안으로 감독기구의 권한이 대폭 확대될 것으로 보이며, 2012년 11월 29일 법안 통과 후 2014년 3월부터 공공 및 민간 기업에 적용 예정

- (배경) 호주 호주 국·내외 프라이버시 이슈 증가와 IT 기술 발달 속도에 호주의 Privacy Act가 적절하게 대처하지 못하자 2008년 호주 법안 개정 위원회(ALRC, An Australian Law Reform Commission¹⁾)에서 관련한 개선안을 권고
 - ALRC는 Privacy Act of 1998을 28개월동안 연구 및 조사하여 74장 295개의 권고안이 담긴 ALRC Report 108을 호주 정부에 제출
 - 이에, 호주정부는 ALRC Report 108 내 295개의 권고안 중 197개를 받아들였으며 이에 따른 Privacy Act 수정안 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012'이 호주 의회에 소개됨
- (주요내용) 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012'에 포함될 내용은 다음과 같음
 - 공공 기관과 일반 기업에 독립적으로 적용되는 프라이버시 원칙이 Australian Privacy Principle (APPs)로 통일
 - 국외이전의 확대에 따라 해외에 기반을 둔 클라우드 서비스 제공자의 데이터 해외 전송에 대한 의무 규정과 프라이버시 위반 시 책임 내용 포함
 - 다이렉트 마케팅시, 특정 요건이 갖춰질 경우에만 고객정보 수집 가능

1) ALRC: 호주의 독립적인 법령 조직으로 호주법률을 검토하고 법률개정을 위한 옵션을 옹호하는 업무를 담당

- 프라이버시 정책의 적극적인 관리와 정기적인 정책 준수 확인 요구
 - 신용평가보고서 제공시 정보에 대한 개정
 - Australian Information Commissioner의 권한 강화 및 벌금 집행권 부여
- (법안 승인 및 발효) 2012년 11월 29일 ‘Privacy Amendment (Enhancing Privacy Protection) Bill 2012’이 승인되었으며 2014년 3월부터 공공기관 및 민간 사업자에게 발효 예정
- (시사점) 개정안이 통과되면 호주 정보 감독원의 권한이 확대될 예정
- 불평사항을 해결하고, 조사를 지휘하고, 프라이버시 컴플라이언스를 증진 시킬 수 있게 권한 확장
 - 프라이버시 법을 준수하기 위한 조치에 대한 기관들의 서면동의서 수락할 수 있는 권한 부여
 - 기관의 특정 프로젝트에 대해서 개인정보 영향 평가를 하도록 지시할 수 있는 권한 부여

[자료출처]

<http://www.alrc.gov.au/publications/report-108>

<http://www.alrc.gov.au/inquiries/privacy>

http://www.claytonutz.com/publications/edition/24_may_2012/20120524/introduction_of_privacy_bill_to_parliament.page

http://www.dpmc.gov.au/privacy/alrc_docs/stage1_austr_govt_response.pdf

<http://www.ag.gov.au/Privacy/Pages/AGD-Privacy-Act-Amendments.aspx>

<http://www.mondaq.com/404.asp?404;http://www.mondaq.com:80/australia/x/197852/Data+Protection+Privacy/Privacy+reforms+pass+House+of+Representatives+What+does+this+mean+for+the+private+sector&login=true>

2 빅데이터와 클라우드 환경에서의 개인정보보호 기반 강화

- ▷ EU 집행위원회, 클라우드 환경에서의 프라이버시 보호 추진방향 제시
- ▷ 아일랜드 데이터보호 감독원, 클라우드 보안 가이드 발행
- ▷ 이탈리아, 클라우드 서비스 이용에 따른 개인정보보호 10대 수칙 발표
- ▷ CSA-후지츠, 빅데이터 작업 그룹 공동 설립
- ▷ ICDPPC, 빅데이터 시대에서의 개인정보 프로파일링 선언문 발표
- ▷ 영국 ICO, 데이터 익명화 실행규칙 제정

EU 집행위원회, 클라우드 컴퓨팅 전략에서의 프라이버시 보호 방향제시

요 약

- 유럽 집행위원회(EC)는 지난 7월, 미래 클라우드 컴퓨팅의 잠재력을 확인하고 프라이버시 보호 추진 방향을 포함한 클라우드 컴퓨팅 전략을 마련하기로 결정
- 클라우드 컴퓨팅 전략을 통해 사용자와 서비스 제공자를 위한 체크리스트를 제공하고 공공 및 일반 기업 사이의 파트너십을 도모할 계획

○ **(배경)** 유럽 집행위원회 (European Commission, EC) Digital Agenda에서 클라우드 컴퓨팅 시장의 잠재력을 예상하고 클라우드 컴퓨팅 전략을 연내 발표

- 클라우드 컴퓨팅 서비스 제공자, 업계 전문가 등이 포함된 working group을 구성, 프라이버시 보호 추진방향을 포함한 클라우드 컴퓨팅 전략 준비

○ **(내용)** 이번 ‘Cloud Computing Strategy’ 초안에는 다음 내용 포함

- 클라우드 컴퓨팅을 개발하는 데 영향을 미칠 수 있는 데이터 보안 및 프라이버시 제도를 검토하고 프라이버시 보호 강화와 명확한 내용을 담은 가이드라인 제정
- 프라이버시 자문기구인 Article 29 Data Protection Working Party (이하 working party 29) 지침을 바탕으로 클라우드 컴퓨팅의 프라이버시 보안과 관련한 다음 사항을 골자로 한 가이드라인 및 권고사항 제공

- (1) 투명성 요구조건의 준수, 클라우드 수집 목적 범위에서 벗어난 사용금지, 계약시 준수해야 하는 정보주체의 보호, 기술적·관리적 보안 정책, 데이터 국외이전, 클라우드 컴퓨팅 서비스 제공자와 사용자의 준수사항
- (2) 클라우드 컴퓨팅 사용이전에 사용자가 위험분석을 하기 위해 필요한 체크리스트 제공
- (3) 클라우드 컴퓨팅 서비스 제공자가 하청업체를 이용에 대한 사용자의 동의 의무와 하청업체의 내용 변경 시, 하청업체 운영자의 변동사항 제공 의무
- (4) ²⁾Safe-harbor를 보완할 수 있는 추가 대책

2) Safe-Harbor 인증: 유럽연합회의 데이터 보호에 대한 지침이 1998년 10월에 발효되어 EU에서 정의하는 적정 프라이버시 보호 기준 수준을 만족하지 않는 나라로의 개인정보 전송이 금지됨. 미국 상무부에서 유럽연합회의와 상의하여 safe-harbor 프레임워크를 만들어 이에 만족하는 기업들은 유럽 연합국과 데이터 전송이 가능

- 클라우드 컴퓨팅 상의 데이터 보안과 가용성 유지를 위한 기술적 표준, 표준 계약서, service level agreement 제시
- (향후 계획) European Cloud Partnership을 통해 공공민간 연합으로 2013년까지 클라우드 컴퓨팅 기술 검증 프레임워크 마련

[자료출처]

<http://www.mondaq.com/404.asp?404;http://www.mondaq.com:80/x/188046/IT+inter-net/European+Commissions+Cloud+Computing+Strategy+For+Europe+To+Be+Released+Shortly&login=true>
<http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50>
<http://www.euractiv.com/infosociety/brussels-unveil-eu-cloud-computi-news-514012>
<http://www.mondaq.com/x/190234/IT+inter-net/Article+29+Working+Party+Analyses+Data+Protection+Issues+Regarding+Cloud+Computing>

아일랜드 데이터보호 감독원, 클라우드 보안 가이드 발행

요 약

- 아일랜드 데이터보호 감독원은 클라우드 보안 관련 가이드를 발행
- 가이드의 내용은 데이터 보안, 데이터 위치, 서면 계약서와 관련된 내용으로 구성됨

○ **(개요)** 아일랜드 데이터 보호 감독원은 2012년 7월, 클라우드 컴퓨팅 서비스시 고려해야할 데이터 보호 이슈에 대한 가이드라인을 개발

- 클라우드 보안과 관련하여 지난 2012년 5월 발행된 EU의 정보보호작업반 (Article 29 Working Party)의 의견서 (Opinion 05/2012) 참고함

○ **(주요내용)** 가이드의 내용은 클라우드의 데이터 보안, 데이터 위치, 서면 계약서와 관련된 내용으로 구성됨

- 클라우드 데이터 보안:

- ▶ 데이터 위탁 시, 개인 데이터 보안의 책임은 데이터 처리자(수탁자)가 아닌 데이터 관리자(위탁자)에게 있음
- ▶ 클라우드 서비스를 이용할 때, 데이터 처리자 (클라우드 제공자)는 데이터 관리자의 지시에 따라 데이터를 처리해야 함
- ▶ 데이터 관리자는 데이터 처리자가 적절한 보안 조치를 하는지 확인해야 함
 - ※ 데이터의 무결성, 접근제어, 보조 처리자, 데이터 유출시 조치, 데이터 관리자가 데이터를 제거, 삭제, 전송할 권리 등의 적절성 등
- ▶ 클라우드 제공자의 직접적 감사(audit) 보다는 승인된 국제표준에 따라 제3자 인증이 이루어지는 것을 확인 하는 것이 더 좋은 보안 방식임

- 클라우드 데이터 위치:

- ▶ 클라우드 고객(즉 데이터 관리자)은 제3국으로의 데이터 이동시 데이터 보호가 “adequate(적절한)” 수준의 나라인지 확인해야 함
- ▶ 데이터 보호가 “adequate(적절한)” 수준의 나라가 아닐 경우 미국

세이프 하버 프로그램, EU형 표준모델계약, BCR(Binding Corporate Rules)을 준수하여 이동되어야 함

- 클라우드 계약서:

- ▶ 개인 데이터를 데이터 관리자가 위임하여 데이터 처리자가 처리할 경우, 데이터 관리자와 처리자는 서면 계약서를 작성해야 함
- ▶ 적절한 클라우드 계약서는 표준화된 데이터 보호 안전보장장치와 상당한 주의와 책임을 촉진할 수 있는 추가적인 메커니즘(감사, 제3자인증 등)을 포함해야 함

[EU 정보보호작업반의 의견서 (Opinion 05/2012)]

- (배경) 클라우드컴퓨팅 서비스는 데이터가 누구에 의해, 어디서, 어떻게 처리되는지에 대한 충분한 정보 제공이 어렵기 때문에, 정보주체가 자신의 개인정보처리에 대해 충분히 고지받기 어렵다는 점을 가장 큰 문제로 지적함
- (주요내용) 작업반은 클라우드컴퓨팅의 정보보호 문제에 대응하기 위해 고려해야 할 사항을 다음과 같이 제시함
 - 클라우드컴퓨팅 서비스를 이용하려는 사업자와 공공기관은 가장 먼저 포괄적이고 철저한 위험분석을 수행하여야 함
 - EEA 내의 모든 클라우드컴퓨팅 서비스 제공자는 이용자가 그 서비스 이용의 장단점을 적절히 평가하기 위해 필요한 모든 정보를 제공해야 함
 - 클라우드컴퓨팅 서비스 이용자는 정보관리자로서의 책임이 있으므로, EU의 정보보호법규 준수를 보장하는 서비스 제공자를 선택해야 함
 - 기술적·관리적 보호조치에 관한 충분한 보장이 서비스제공자와 이용자간 계약에 반영되어야 함
 - 클라우드컴퓨팅 서비스 이용자는 서비스제공자가 국외이전의 합법성을 보장하는지를 반드시 확인해야 함

[자료출처]

<http://www.mondaq.com/x/196732/data+protection/Data+Protection+Commissioner+Looks+To+The+Clouds>

<http://www.cloudstrong.ie/blog/?cat=5>

<http://lugenzhe.blog.me/90148074114>

이탈리아, 클라우드 컴퓨팅 이용에 따른 개인정보보호 10대 수칙 발표

요 약

- 이탈리아 데이터 보호 기관은 클라우드 컴퓨팅 서비스를 사용하는 데 있어서 개인 정보 처리에 대한 10가지 수칙을 마련하여 가이드 형태로 제공

○ **(개요)** 2012. 8월, 이탈리아 데이터 보호 기관은 클라우드 컴퓨팅 서비스 수요 증가에 따라 사용자들에게 개인 정보 보호와 관련하여 클라우드 컴퓨팅 사용에 대한 가이드 제공

○ **(주요 내용)** 클라우드 컴퓨팅 서비스 사용에 대해 다음 10가지의 주요 규칙 제공

- (1) 클라우드 컴퓨팅 서비스 제공자의 신뢰도, 서비스 제공 경험, 적절한 기술적 환경 보유 여부 확인
- (2) 상이한 클라우드 컴퓨팅 시스템 환경 사이에 호환성을 높이기 위한 데이터에 대한 기준과 형식 정보 필요
- (3) 클라우드 서비스의 가용성 보장과 언제든지 데이터에 접근할 수 있는 권한 확보
- (4) 클라우드에 저장하는 데이터의 성격과 민감성에 대한 적절한 주의가 필요
- (5) 클라우드 컴퓨팅 서비스 품질에 대한 지속적인 모니터링
- (6) 클라우드 컴퓨팅 서비스 제공자의 데이터 저장 위치가 지역 내, 혹은, EU 연합국 내, 혹은 유럽 외 지역인지 사전 확인 필요
- (7) 클라우드 서비스 제공에 대한 계약 이용 약관의 꼼꼼한 검토 필요
- (8) 클라우드상의 데이터 저장 기간과 말소에 대한 명확한 의무 사항 정의 필요
- (9) 데이터의 기밀성 보장을 위해 적절한 데이터 보호 조치 존재 여부를 사전에 확인
- (10) 클라우드 컴퓨팅 제공사 및 사용자 기업 직원들을 대상으로 데이터 처리에 대한 교육 및 훈련 필요

[자료출처]

<http://www.mondaq.com/x/193388/data+protection/Italian+DataProtection+Authority+Provides+Guidance+For+Cloud+Services>

CSA, Fujitsu, Big Data Working Group 설립

요 약

- Cloud Security Alliance와 Fujitsu Laboratories of America 등에서 빅데이터 보안 이슈에 대한 연구를 위해 Big Data Working Group 설립
- Big Data Working Group에서는 빅데이터의 보안 및 프라이버시 연구, 표준 개발에 초점을 둘 예정

- (개요) Cloud Security Alliance (이후 CSA)와 Fujitsu Laboratories of America (이후 Fujitsu) 등 30여개사가 Big Data Working Group (이후 BDWG)를 설립

※ CSA: 클라우드 컴퓨팅 보안을 제공하는데 초점을 둔 비영리 단체

Fujitsu: 통신네트워크와 IT기반의 사회 인프라 구축을 지원하는 정보통신기술 전문업체

- (내용) BDWG에서 빅데이터의 보안과 프라이버시 연구 및 표준개발에 중점을 둘 예정이며 다음의 목표방향 설정

- 빅데이터 보안과 개인정보보호를 위한 베스트 프랙티스 수립을 목표
- 업계와 정부가 이들 베스트 프랙티스를 적용할 수 있도록 지원
- 빅데이터 보안과 개인정보보호 표준들에 영향을 끼칠 수 있도록 표준 개발 조직들과 협력 관계를 구축
- 보안과 개인정보보호 이슈에 초점을 맞춘 새로운 연구 적용 가속화

- (향후 계획) 2012년 말까지 업계와 관계부처 등으로부터 자본마련후 추진

[BDWG가 제시한 Big Data 기술의 주요 이슈]

- 빅데이터가 소셜 네트워크, 모바일 단말기 등을 포함해 여러 경로의 단말기로부터 수집되므로, 현 기술과 근본적 차별성이 있음
- 데이터에서 정보는 안전하게 수집 및 재배포 되어야 하며, 정형화되고 이해하기 쉬운 프레임워크 환경 내에 있어야 함
- 빅데이터 관리 시스템이 대량의 정보들, 그 중 대다수는 사용되지 않는 정보들을 수집하므로 데이터 필터링이 중요
- 빅데이터를 활용하려는 조직에서는 데이터 소유자, 제공자, 사용자가 분리되는 특징이 있으며, 따라서 외부로부터 데이터 무결성을 막을 수 있는 방법을 모색해야 함

[자료출처]

<http://www.techweekeurope.co.uk/news/fujitsu-ebay-lead-big-data-privacy-research-group-91223>

ICDPPC, 빅데이터 시대에서의 개인정보 프로파일링 선언문 발표

요 약

- 우루과이에서 제34회 개인정보보호감독기구 국제회의 개최, 빅데이터 시대에서의 개인정보 프로파일링 선언문 발표
- 본 선언문에서는 빅데이터에 기반한 대용량 데이터베이스 분석이나 프로파일링의 개인정보보호 문제를 극복하기 위한 8개 항목 제시

○ **(배경)** 2012년 10월, 우루과이에서 제34회 개인정보보호감독기구 국제회의 (International Conference of Data Protection and Privacy Commissioners, 이후 ICDPPC)가 개최되었으며, 프로파일링에 대한 위험성을 다음과 같이 제시

- 빅데이터에 기반한 대용량 데이터베이스 분석이나 profiling은 각 기관이나 기업에서 표적처리(target process)를 위한 위험 분석을 수행하게 되면 개인정보보호 차원에서 우려
- 이러한 문제를 극복하기 위하여 목적제한의 원칙을 비롯한 개인정보보호의 원칙들과 각각의 과정을 판단할 수 있는 프레임워크를 재확인 필요

※ 각국의 개인정보보호 감독기구 연합체인 ICDPPC는 국제적으로 새롭게 대두되는 프라이버시 및 개인정보보호 현안을 논의하고 관련정보 교류 및 국제협력을 위하여 매년 회의를 개최

○ **(8개 항목)** 프로파일링에 관한 우루과이 선언문에서 제시한 8개 항목

- 신뢰형성을 위하여 profiling의 최대 가능 범위(maximum possible extent)에 대하여 공지하여야 하며 profiling의 수집방법과 수집목적 명시를 통해 투명성을 제고해야 함
- profiling 사용의 필요성 설정 명확화, 어떤 가정(assumption 또는 algorithm)과 data를 기본으로 profiling을 할지 결정, 프로파일 적용 방법 결정

※ 이상의 3가지 단계는 각각 별도로 결정하여야 하며 법적 관리감독 병행 요구

- 프로파일과 이행 알고리즘을 지속적으로 확인(continuous validation)하기 위하여 적절한 통제 필요

- 알고리즘의 증가된 효율성이 주는 위험성에 대비하기 위해 profiling 운영 시에 인위적인 조율필요
- 프로파일을 생산한 정보와 실제 적용사이의 균형 유지
- 개인정보처리자는 프로파일 활용시 정보주체의 프라이버시 권한을 보호해 줄 수 있는 관련 대책 마련
- 공공 및 민간의 영역을 모두 포함하는 감독권한을 가진 강력하고 독립적인 실행기구(privacy enforcement authorities, PEA) 필요
- 실행기구(privacy enforcement authorities, PEA)에게 회계감사 등 정부의 계획을 관리 감독할 수 있는 권리 부여

[자료출처]

<http://www.mondaq.com/canada/x/206410/data+protection/Big+Data+And+Cloud+Computing+Meet+The+Uruguay+Conference+Of+Data+Protection+Authorities>

<http://lugenzhe.blog.me/90158193754>

영국 ICO, 데이터 익명화 실행 규칙 제시

요 약

- 영국 정보위원회(ICO)는 데이터 익명화에 대한 실행 규칙 (Code of Practice) 및 사례연구와 good practice를 제공할 Anonymization Network를 발표
- 빅데이터 시대에서 프라이버시 보호와 동시에 유용성도 확보될 것으로 기대되며, 향후 관련 웹사이트를 개설하여 관련 정보 및 가이드라인 제공 예정

○ (배경) 2012년 11월 20일, 영국 정보 위원회 (ICO, Information Commissioner's Office)는 Data Protection Act 1998를 기반으로 한 데이터 익명화 실행 규칙 제시

- 개인 프라이버시를 보호하면서 풍부한 데이터 자원의 유용성 확보를 위해 데이터 익명화 실행 규칙을 준비

○ (주요 내용) 데이터 익명화 실행 규칙은 "Anonymization: managing data protection risk code of practice" 라는 이름으로 발간되었으며 주요 내용은 다음과 같음

- 익명화된 개인 데이터는 더 이상 개인정보로 취급되지 않음. 이것은 정보가 (de-anonymization)시에도 동일하게 적용됨
- 기술적인 주요 이슈는 개인 정보를 재식별 (re-identify)하기 위해 익명화된 데이터가 제 3 자가 제공한 정보와 결합될 수 있는 지 여부임
- 재식별의 위험을 평가하는 데 있어서, ICO는 "motivated intruder³⁾" 테스트를 사용할 것을 권고
- 데이터 재식별의 위험과 민감도 정도에 따라 데이터 사용 제한에 대한 명확한 기준을 마련해야 함
- 데이터 익명화에 대해서 Data Protection Act에 따른 개인의 동의는 요구되지 않으나 기관은 프라이버시 정책에 데이터 익명화 가능성에 대해 언급해야 함

3) motivated intruder test: 데이터 자원에 접근 가능하고 사전 지식은 없지만 데이터 식별을 원하는 자가 조사기법으로 데이터를 de-anonymize 할 수 있는 지 여부를 테스트 하는 것

- 그러나 만일 기관이 재식별을 통해 개인 정보를 수집한다면 해당 기관은 관련 정보를 제공하고 동의서를 받아야 함
- (향후 계획) ICO는 익명화 실행 규칙과 함께 "Anonymization Network (www.ukanon.net)" 웹사이트를 오픈하여 온라인 사용자에게 데이터 보호 규정 및 가이드라인 변경에 대한 정보를 제공할 예정임

[자료출처]

<http://www.mondaq.com/x/207776/data+protection/Data+Anonymization+UK+Code+and+a+New+Anonymisation+Network>

http://www.ico.gov.uk/news/latest_news/2012/~media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Practical_application/anonymisation_code_summary.ashx

<http://www.zdnet.com/ico-publishes-code-of-practice-for-anonymizing-data-7000007791/>

3

모바일환경 보편화와 위치정보·스마트폰 관련 조치 확대

- ▷ 프라이버시 미래 포럼, 모바일 앱 조사 연구 결과 발표
- ▷ 美 이통사, FCC 프라이버시 강화 반대 입장 표명
- ▷ 美 캘리포니아주 의회, 위치 프라이버시 법안 통과
- ▷ 美 FTC, 앱 개발자들을 위한 가이드 제공
- ▷ 캐나다 프라이버시 위원회, 앱 개발 가이드라인 제시
- ▷ ACT, 앱 프라이버시 아이콘 개발 보급
- ▷ 美 FCC, 스마트폰 이용자를 위한 보안 가이드 발표

美 프라이버시 미래 포럼, 모바일 앱 조사 연구 결과 발표

요 약

- 2012년 7월 11일, The Future of Privacy Forum은 “FPF 모바일 앱 연구” 보고서 발표
- 아이폰, 구글, 킨들 등 3개의 대표적인 앱스토어 플랫폼에서 각각 25개의 무료앱과 25개의 유료앱을 대상으로 프라이버시 정책 제공 조사 실시

- (개요) 시민단체 The Future of Privacy Forum (이후 FPF)이 2012년 7월 11일, “FPF 모바일 앱 연구 (June 2012 FPF Mobile Apps Study” 보고서를 발표
- (조사대상) FPF는 2012년 6월, 3개의 대표적인 앱스토어 플랫폼에서 각각 25개의 무료앱과 25개의 유료앱을 대상으로 조사 실시
 - 3개의 앱스토어 플랫폼은 iOS App Store (이후 iStore), Goolge Play (이후 Google Store), Kindle Appstore (이후 Kindle Store)임
- (연구내용) 프라이버시 정책을 제공하는 앱 개발자들이 증가하는 추세이며 무료앱 보다 유료앱의 경우가 정보 제공률이 더 높은 것으로 조사
 - iStore, Google Store, Kindle Store의 150개의 앱 중 61.3%가 프라이버시 정책정보 제공
 - 유료 앱의 69.3%, 무료 앱의 53.3%가 프라이버시 정책 제공
- ※ 전년도 조사 대비, iStore에서 프라이버시 정책이 있는 무료 앱이 40%에서 84%로, 유료 앱의 경우 60%에서 64%로 증가, Google Store에서 프라이버시 정책이 있는 무료 앱이 70%에서 76%로, 유료 앱의 경우 30%에서 48%로 증가
- 프라이버시 정책에 대한 접근 방법 중 대부분 링크 방법으로 제공
 - Google Store와 iStore의 무료 앱중 22.7%와 유료 앱의 20%가 앱스토어의 프로모션 페이지에서 프라이버시 정책 다운로드 가능

- 무료 앱의 48%와 유료 앱의 32%가 앱자체에서 또는 앱에 포함된 링크를 통해 프라이버시 정책에 접근 가능
 - 앱에서 프라이버시 정책이 접근 가능하지 않을 경우 이용자들은 프라이버시 정책을 찾기 위해 웹을 통해 검색 필요
- (주요 이슈) FPF는 위치정보와 같은 민감한 개인정보를 수집함에도 불구하고, 아직 프라이버시 정책을 제공하지 않는 개발자들도 다수 존재하고 있음을 확인
- iStore의 50개의 앱 중 12개가 상세한 위치 정보를 요구 하였고, 그 중 10개의 앱이 프라이버시 정책 제공, Google Store의 50개 중 14개의 앱이 상세한 위치정보를 요구하였고, 그 중 10개의 앱이 프라이버시 정책 제공
- FPF는 소수의 앱들이 가독성이 좋은 짧은 알림 형태로 프라이버시 정책을 제공하기 시작하고 있음을 강조
- ※ 조사 대상 앱들 중, Zynga라는 개발자가 만든 6개의 앱들이 이와 같은 형태로 프라이버시 정책 제공

[자료출처]

<http://bits.blogs.nytimes.com/2012/07/12/mobile-app-developers-scoop-up-vast-amounts-of-data-reports-say/>

<http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf>

<http://www.futureofprivacy.org/2012/07/11/fpf-study-results-show-app-developers-heed-call-for-privacy-policies/>

미 이통사들, FCC의 프라이버시 강화에 반대 입장 표명

요 약

- 미국 내 무선 이동통신 사업자들은 FCC (Federal Communication Commission)를 상대로 프라이버시 강화 정책 적용 우려 표명
- 미국 무선사업협회 CTIA (Cellular Telephone Industry Association)에서는 FCC는 법적 규제 권한이 부족하다는 의견
- 이에 상무성의 NTIA (The National Telecommunications and Information Administration)는 프라이버시 보호를 위한 자발적인 행동강령 제정 준비

○ **(배경)** 대다수 이동통신 사업자들이 Carrier IQ라는 소프트웨어를 통해 고객들의 휴대전화 사용정보를 저장하고 있다는 것이 밝혀짐

※ Carrier IQ : 사용자의 사용이력 (예. 통화기록, 위치, 키입력 등)을 기억하는 소프트웨어로 현재 Android, BlackBerry, iOS 등 전세계 1억 4,000만대의 스마트폰에 설치된 것으로 추산

○ **(FCC 대응)** FCC는 의사록을 통해 휴대전화 사용자들의 개인정보보호를 위해 이동통신사들의 책임과 의무에 대한 공청을 받음

[FCC 의사록]

o Communication Act 섹션 222의 정보통신 사업체의 고객정보 기밀 유지 의무를 바탕으로 다음 사항에 대한 공청을 받음;

- (1) 서비스 제공자에 의해서만 휴대기기가 판매되어야 하는 지 여부
- (2) 휴대기기를 설정을 잠가서 오로지 특정 서비스 제공자의 통신망상에서만 사용되도록 할 것인지 여부
- (3) 정보수집 및 저장하는 소프트웨어의 설계, 통합, 설치 사용에 대한 통제수위
- (4) 휴대기기 내 운영체제, 미리 설치되는 소프트웨어, 보안기능의 선택, 통합, 업데이트에 대한 서비스 제공자의 역할의 정의
- (5) 수집된 정보의 사용 방법
- (6) 음성서비스 혹은/그리고 데이터 서비스에 관련된 정보 포함 여부

- (업계 반응) 무선이동통신 사업자들은 FCC의 프라이버시 정책 강화 휴대전화 사용자들의 프라이버시 보호강화를 위한 정책 수정을 반대
- 이동통신 사업자들은 Carrier IQ 사용규제가 서비스 품질 저하를 낳을 수 있다는 의견을 제시
 - Verizon 과 AT&T는 FCC는 콘텐츠 규제 법적 권한이 없으며 이동통신회사의 자발적인 고객 프라이버시 보호정책이 더 효과적이라고 밝힘
 - AT&T는 추가적으로 특정 업체에 국한되지 않고 이동통신 서비스 제공자 뿐만 아니라 이동통신 기기 제조자·운영시스템·검색엔진·소셜 네트워크 사업자 등 모든 업체에게 동일한 정책이 적용되어야 한다고 주장

[자료출처]

<http://thehill.com/blogs/hillicon-valley/technology/238059-cellphone-carriers-warn-fcc-not-to-regulate-privacy>

http://www.multichannel.com/article/487259-CTIA_FCC_Has_No_Roving_Mandate_to_Protect_Info_Stored_on_Mobile_Devices.php

http://www.broadcastingcable.com/article/487251-CTIA_FCC_Has_No_Roving_Mandate_to_Protect_Info_Stored_on_Mobile_Devices.php

<http://www.fcc.gov/document/privacy-and-security-information-mobile-devices>

<http://www.jdsupra.com/legalnews/jdsupra-03541/>

캘리포니아州 의회, 위치 프라이버시 법안 통과

요 약

- 2012년 8월 22일, 캘리포니아주 의회는 사건 용의자 휴대전화의 위치 데이터 수집시 사전 영장 요구토록 하는 Location Privacy Act of 2012 (SB-1434) 의결
- 일부기관 및 주지사의 반대로 해당 법안 통과 여부 주목

- (추진배경) 2012년초 미국시민자유연합 (ACLU, American Civil Livity Union)에 따르면 법집행기구에서 휴대폰 추적에 필요한 영장청구 기준의 상이함을 문제로 제기

- 현재 관련법이 마련되어 있지 않아 미국 내 법집행기구는 영장없이 휴대전화 위치 데이터를 이동통신회사에게 요구 가능

※ ACLU : 인권과 언론의 자유옹호를 위한 비영리 단체로 1920년에 설립

- (법안제안) 샌프란시스코 상원의원인 Mark Leno는 영장 없는 휴대폰 추적에 따른 프라이버시 침해 우려를 표명하면서 Location Privacy Act of 2012 (SB-1434)를 상정하고 의회 통과

[Location Privacy Act of 2012 (SB-1434) 주요 골자]

1. 전자 기기 상의 위치 데이터를 수집하기 위해 사전 영장을 필요로 함
2. 영장 기간은 30일로 제한하며 판사의 허가 하에 추가 30일 연장 가능
3. 다음과 같은 상황에서는 영장 없이 위치 데이터 수집 가능;
 - (a) 응급 전화에 대한 대응
 - (b) 휴대기기의 소유자와 사용자가 다를 때, 소유자로부터 승인
 - (c) 만약 사용자가 사망했거나 실종 시, 법적 대리인이나 친척으로부터 동의
 - (d) 응급상황에 사용자가 죽음이나 부상과 같이 생명에 위협을 느끼는 상황이라고 판단 시
4. 48시간 이내 응급상황 하에 위치 데이터 획득에 대한 보고서를 제출

- **(반대의견)** 캘리포니아 주지사 Jerry Brown이 2011년 비슷한 법안에 거부권을 행사한 적이 있어 이번 법안을 통과시킬지 여부가 주목
 - 또한, 미국 무선사업협회 (CTIA, Cellular Telephone Industry Association)은 위치 추적 데이터를 법 집행기구에 제출하는 데 따른 업무 부담이 예상돼 해당 법안 반대

[자료출처]

<http://arstechnica.com/tech-policy/2012/08/california-state-legislature-approves-location-privacy-act/>

<http://www.zdnet.com/california-approves-location-privacy-act-get-a-warrant-7000003050/>

<http://www.infosecurity-magazine.com/view/27753/californias-location-privacy-bill-passes-assembly/>

http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1401-1450/sb_1434_bill_20120807_amended_asm_v94.html

<https://www EFF.org/file/34734#page/1/mode/lup>

미국 FTC, 앱 개발자들을 위한 가이드 제공

요 약

- 미국 FTC는 신규 앱 마케팅 진행 시 요구되는 프라이버시 기본 원칙과 광고의 진실성(truth-in-advertising) 준수 내용이 담긴 가이드를 출간
- 가이드를 통해 앱 개발자들의 프라이버시 원칙에 대한 인식 수준을 높일 수 있을 것으로 기대

○ **(배경)** 앱 비즈니스가 활성화 되고 있으나 앱 개발자 및 소규모 앱 개발 회사들은 앱 개발에 따른 수익 창출을 이루지 못하고 있는 실정

- 이에 FTC는 truth-in-advertising 표준과 기본 프라이버시 원칙 준수를 돕고자 가이드 출간하면서 본 가이드 준수가 이익창출에 도움줄 것으로 언급

○ **(주요 내용)** ‘Marketing Your Mobile App: Get It Right from the Start’ 가이드에서 제시하는 8가지 가이드라인은 다음과 같음

- (1) 개발하는 앱의 기능에 대한 설명을 제공할 것
- (2) 앱의 주요 정보를 명확하고 이해하기 쉽게 제공할 것
- (3) 앱 개발 초기부터 프라이버시를 고려할 것
- (4) 사용자가 쉽고 편리하게 이용할 수 있는 앱을 개발하고 고객의 선택을 존중할 것
- (5) 프라이버시 보호 약속을 지킬 것
- (6) 어린이용 앱 개발 시, 어린이 프라이버시를 보호할 것
- (7) 민감한 정보 수집 시 반드시 사용자 동의를 얻을 것
- (8) 사용자 데이터를 안전하게 보관할 것

○ **(기대 효과)** 앱을 통한 데이터 수집, 활용, 공유 기능을 개발자들이 결정하는 만큼 본 가이드를 통해 프라이버시 기준과 개발자 의무사항의 이해수준 제고 기대

[자료출처]

<http://www.ftc.gov/opa/2012/09/mobileapps.shtm>

<http://business.ftc.gov/documents/bus81-marketing-your-mobile-app>

캐나다 프라이버시 위원회, 앱 개발 가이드라인 제시

요 약

- 캐나다 알버타주와 브리티시컬럼비아주 프라이버시 위원회는 모바일 애플리케이션에 대한 공동 가이드라인 제시
- 가이드라인은 현재 마련된 프라이버시 관련 규정 내 프라이버시 원칙을 쉽고 간단하게 요약

- **(개요)** 2012년 10월 말, 캐나다의 알버타주와 브리티시컬럼비아주의 프라이버시 위원회는 "Seizing Opportunity: Good Privacy Practice for Developing Mobile Apps" 라는 이름으로 앱 개발 가이드라인 제시
- **(내용)** 프라이버시 위원회는 모바일 앱 환경과 관련하여 좀 더 의미있는 프라이버시 관련 동의를 구하는 데 다음과 같은 권고안을 제시
 - Layering Information: 프라이버시 공개에 대한 약관을 icon, label 그리고 image로 제공하고 링크를 통해 좀 더 자세한 정보를 제공할 것
 - Privacy Dashboards: 프라이버시 설정 기능을 사용자에게 제공하여 사용자에게 프라이버시 보호 관련 선택권한을 부여할 것
 - Color and sound: 정보의 민감도나 결정에 대한 중요도 정도를 색깔이나 사운드로 표시할 것
 - Timing of user notice and consent: 사용자가 쉽게 접근하고 이해하기 쉬운 앱 프라이버시 정책을 제공할 것
- 또한 프라이버시 위원회는 특정 유형의 개인 정보의 수집과 사용에 대한 좀 더 구체적인 가이드라인을 다음과 같이 제시
 - Sound, location and movement: 모바일 기기의 위치 및 이동센서로부터의 음성과 데이터 수집 및 이용에 대해서는 모바일 앱 기능과 직접적으로 연관이 있어야 하고 사용자 동의를 구해야 함

- Cameras: 모바일 기기 카메라 활성화가 필요한 앱의 경우, 사용자의 동의를 구해야 함
 - Third party: 모바일 기기 내 연락처 정보와 같이 제 3 자의 정보는 사용자 동의 없이 수집 금지
- (기대 효과) 사용자에게는 어떤 앱을 신뢰할 수 있고 지속적으로 사용할 수 있는지에 대한 이해 증진과 개발자에게는 프라이버시 관련 투명성과 공개 그리고 동의 절차의 중요성에 대한 인식 제고 기대

[자료출처]

http://www.priv.gc.ca/information/pub/gd_app_201210_e.asp

ACT, 앱 프라이버시 아이콘 출시

요 약

- 美 경쟁기술연합(ACT)은 앱 신용 프로젝트의 일환으로 앱 프라이버시 아이콘 개발
- 앱 프라이버시 아이콘은 사용자에게 앱이 광고, 데이터 수집, 소셜 네트워크와의 데이터 공유 등 정보를 제공

○ **(개요)** ACT는 지난 몇 개월간 어린이 앱 개발자들과 함께 아이콘을 제작해 왔으며, 아이콘의 지속적 개발을 위해 Moms With Apps, PrivacyChoice.org, Operatio Apps.의 대표들과 함께 자문위원 구성

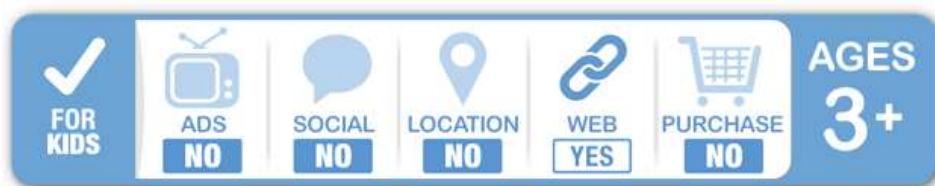
- 이에 지난 2012년 10월, 경쟁기술연합 (Association for Competitive Technology, 이후 ACT)이 앱 프라이버시 아이콘을 출시

○ **(내용)** 앱 프라이버시 아이콘은 사용자에게 앱이 광고, 데이터 수집, 소셜 네트워크와의 데이터 공유 등 유무를 알려주는 역할

- 아이콘은 프라이버시 고려사항을 알려주며, 프라이버시 정책을 교체하기 보다는 존재하는 프라이버시 정책의 효율성을 증가시키는 기능

- 아이콘은 앱 웹사이트, 앱 자체, 앱 스토어 문서 등 여러 가지로 적용 가능

[예시]



○ **(향후 계획)** ACT는 개발자를 위한 오픈소스 코드를 개발할 생각이며, 소셜미디어, 광고 등을 통해 이러한 도구의 홍보 캠페인을 벌일 예정임

[자료출처]

<http://www.eweek.com/developer/act-launches-app-privacy-icons/>

<http://apptrustproject.com/>

美 FCC, 스마트폰 이용자를 위한 보안 가이드 발표

요 약

- 2012년 12월, FCC는 “Smartphone Security Checker”라는 온라인 툴 배포
 - 스마트폰 이용자들이 기기를 도난당하거나 바이러스에 감염 당했을 경우 개인정보 유출을 막는 10단계 권고사항 포함
- (개요) 2012년 12월, 미국 연방 통신 위원회 (Federal Communications Commission, 이후 FCC)가 스마트폰 이용자를 위한 보안 가이드를 발표
- FCC는 “Smartphone Security Checker”라는 OS별 온라인 툴 배포를 통해 스마트폰 이용자들이 기기를 도난당하거나, 바이러스에 감염 당했을 때, 개인정보 유출을 막는 10단계 권고사항을 발표
 - U.S. Department of Homeland Security, FTC, National Cyber Security Alliance, CTIA (무선 산업 무역 협회) 등의 여러 기관에서 협업하여 초안 검토
- (주요내용) FCC의 스마트폰 보안을 위한 10단계
- 1단계: PIN과 암호를 설정하라.
바탕화면에 암호와 개인식별번호(Personal Identification Number, PIN)를 설정하여 1차 방어선이 될 수 있도록 해야 함
 - 2단계: 스마트폰의 보안 설정을 수정하지 말라.
편의를 위해 보안 설정을 수정하지 말 것. 공장에서 일괄화된 보안 설정을 바꾸거나, 탈옥·루팅 등은 외부 공격에 취약성을 가중
 - 3단계: 데이터 백업을 하라.
연락처, 문서, 사진과 같은 데이터를 컴퓨터, 저장공간, 클라우드 등에 저장하여 폰 분실 또는 데이터 유실시 복구 대비
 - 4단계: 믿을 수 있는 소스로부터 앱을 설치하라.
앱을 다운로드 받기 전에 앱 제공자가 합법적인 근원지인지 체크
 - 5단계: 앱의 여러 허락 요청을 무조건 수락하지 말고 먼저 이해할 것
앱이 개인정보를 요청하거나, 모바일폰의 설정들을 변경하는 허가요청을 수락하기 전에 유심히 살펴봐야 함

- 6단계: 원격으로 위치를 찾아주거나 데이터를 지워주는 보안 앱을 설치하라
GPS가 꺼져 있더라도, 원격으로 위치를 찾아주고 데이터를 삭제해 주는 보안 앱을 설치할 것
- 7단계: 스마트폰 소프트웨어의 업데이트와 패치 설치를 반드시 하라
스마트폰의 운영체제 및 소프트웨어를 최신으로 유지함으로써 사이버 공격의 위험을 줄일 수 있음
- 8단계: 공용 Wi-Fi 네트워크 사용시 주의를 기울일 것
공개된 Wi-Fi 네트워크의 사용을 가급적 제한하고, 부득이하게 사용 시 민감한 자료의 접근을 제한, 웹링크 연결, 계좌로그인 정보의 입력시 주의를 기울일 것
- 9단계: 사용하던 스마트폰을 기부하거나, 판매하거나, 재활용할 때, 데이터를 완전히 삭제하라.
사용하던 스마트폰을 다른 사람에게 보낼 때, 개인정보를 완전히 지우고 공장 초기화하여야 함
- 10단계: 스마트폰 도난시 신고하라.
주요 무선 서비스 제공자들과 FCC는 도난 모바일폰 데이터베이스를 운영하고 있으며, 스마트폰 도난시 이를 신고하여 무선 네트워크 비활성화 되도록 조치

[자료출처]

http://www.pcworld.idg.com.au/article/445137/fcc_issues_security_guidance_smartphone_users/

<http://www.fcc.gov/smartphone-security>

http://www.fcc.gov/sites/default/files/smartphone_master_document.pdf

4 얼굴인식기술의 발달과 영상정보처리기기의 규제 강화

- ▷ 영국 ICO, 사우샘프턴 의회에 차량 내 음성녹음 금지 명령
- ▷ 페이스북의 Photo Tag Suggest 기능에 대한 제재 움직임 확산
- ▷ 위키리크스, 미국 정부의 대테러 소프트웨어 사용 폭로
- ▷ 美, 무인 항공기에 대한 프라이버시 보호 법안 제안
- ▷ 美 FBI, 차세대 얼굴 인식 시스템 도입
- ▷ 美 FTC, 프라이버시 관련 얼굴인식기술 사용 가이드라인 제시

영국 ICO, 사우샘프턴 의회에 차량 내 음성녹음 금지 명령

요 약

- 2012.7월 영국정보위원회 (ICO, Information Commissioner's Office)는 택시에 설치된 CCTV가 Data Protection Act를 위반하고 개인데이터를 불공정하게 위법적으로 처리됨을 결정, CCTV를 통한 음성 녹음 금지 명령 조치

- **(배경)** 2009년 사우샘프턴주는 일반 택시 및 콜택시에 CCTV 및 마이크를 설치하여 운전자와 승객의 영상과 대화 내용을 녹화 및 녹음할 것을 택시 면허 발급 조항으로 추가
- **(조치사항)** 그러나, 영국정보위원회는 지난 7월, 'Data Protection Act'와 'European Convention on Human Rights (ECHR)'에 근거하여 사우샘프턴의 해당 내용을 프라이버시 위반으로 결정
 - 7월 25일, 영국정보위원회는 사우샘프턴이 택시 내 영상 및 음성 녹음 통해 개인정보를 불법적으로 처리한다고 밝히며 다음과 같은 조치를 2012년 11월 1일까지 취할 것을 명령 (지금까지 녹음된 음성데이터 중 개인정보는 모두 삭제할 것, 추가적이 개인 정보를 저장 금지)
- **(대응 상황)** 7월 26일, 사우샘프턴 의회는 저장된 영상 및 음성은 사고 조사 증거로만 사용되며 CCTV 설치의 폭력 발생을 억제할 수 있는 가치있는 조치로 판단, ICO에 항소의견 제출
 - ※ 항소에 대한 결론은 2013년 봄에 나올 것으로 예상

[자료출처]

<http://www.techweekeurope.co.uk/news/ico-cab-cctv-87242>

http://www.ico.gov.uk/news/latest_news/2012/council-ordered-to-stop-unlawful-recording-of-taxi-passengers-conversations-25072012.aspx

<http://www.legislation.gov.uk/ukpga/1998/29/contents>

http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/CONVENTION_ENG_WEB.pdf

<http://www.bbc.co.uk/news/uk-england-hampshire-19290688>

페이스북의 Photo Tag Suggest 기능 제재 움직임 확산

요 약

- 독일 데이터 보호 기관에서 페이스북의 얼굴 인식 기술에 대한 조사를 실시
- 얼굴 인식 기능을 통해 수집된 모든 데이터의 삭제, 사용자들에게 얼굴 인식 기능 사용과 데이터 수집에 대한 명확한 동의를 받도록 명령

○ **(배경)** 2012년 8월 15일, 함부르크 데이터 보호 기관은 사용자의 사전 동의 없이 ‘얼굴 인식 기능’을 도입한 페이스북의 Photo Tag Suggest 기능 조사 결정

※ Photo Tag Suggest : 이용자가 페이스북에 올리는 사진을 얼굴 인식 소프트웨어를 통해 분석하여 사진 속 얼굴을 페이스북 이용자와 자동적으로 매치 시키는 기능

- 2012. 3월, 유럽 집행위원회 프라이버시 보호 자문 패널인 Article 29 Working Party는 사용자 동의 없이 생체 데이터 수집은 불법이며 유럽연합회의의 프라이버시 보호법을 위반한 것이라고 판단

○ **(대응 상황)**

- 2012년 9월말, 독일은 수집된 얼굴 인식 데이터를 삭제하고 생체 데이터 수집 시 사용자 동의를 받도록 웹사이트 수정 지시

※ 노르웨이 데이터 보호 위원회는 페이스북의 Facial Recognition 기능의 상세알고리즘과 데이터베이스 내 저장 내용 조사를 위한 조사 설문지 전달 예정

○ **(향후 계획)** 독일의 경우, 추후 페이스북이 데이터 보호 기관의 공식 요청에 따르지 않으면 벌금 부과 및 법정소송 대응 예정

[자료출처]

<http://www.zdnet.com/facebook-must-destroy-facial-recognition-data-or-get-users-approval-germany-decides-7000002720/>

<http://www.4-traders.com/FACEBOOK-INC-10547141/news/Germany-Reopens-Probe-Into-Facebook-s-Face-Recognition-Tool-14463370/>

<http://www.post-gazette.com/stories/business/technology/germany-reopens-facebook-privacy-inquiry-649070/>

<http://www.scmagazine.com.au/News/312466.facebook-facial-recognition-facing-fresh-investigation.aspx>

<http://www.rte.ie/news/2012/0730/data-comm-to-make-facebook-decision-by-october.html>

WikiLeaks, 미국정부의 대테러 소프트웨어 사용 폭로

요 약

- WikiLeaks가 유출된 Stratfor의 이메일을 공개하면서, 미국정부가 대테러 소프트웨어 'TrapWire'를 이용하여 시민을 감시하려 한다고 주장
- 공개된 문건에 따르면, TrapWire가 이미 미전역과 해외의 주요도시들에서 사용 중이나, 미국 정부는 감시의혹 부인

- (개요) WikiLeaks가 2012년 8월 12일, 유출된 Stratfor의 이메일을 공개하면서, 미국정부가 대테러 소프트웨어 'TrapWire'를 이용하여 시민을 감시하려 한다고 주장
 - TrapWire는 2004년, 전직CIA요원들이 설립한 Abraxas Coporation에서 개발한 시스템
 - TrapWire의 기능은 안면인식 기술을 이용하여 CCTV를 통해 사람과 차량 정보를 수집, 중앙 데이터베이스에 저장
- (내용) 공개된 문서에 따르면, TrapWire가 이미 미전역과 해외의 주요 도시들에서 사용 중임
 - 문건에 따르면, 미 국토안보부가 83만 2000달러를 들여 워싱턴 DC, 시애틀 등에 TrapWire를 설치 (뉴욕 지하철에 감시카메라 500개 설치)
 - WikiLeaks는 미국 주요 도시(라스베이거스, 로스앤젤레스, 텍사스주 등)들과 국외(영국 런던, 캐나다)에 이미 설치되었다고 주장
- (대응) 미국정부는 TrapWire의 시민 감시 의혹에 대해 부인
 - 당국은 2011년, 워싱턴 DC, 시애틀의 TrapWire 설치 계약을 해지하였다고 밝힘
 - 뉴욕 경찰 대변인, 뉴욕 지하철 감시카메라 설치에 대해 부인

[참고기사]

<https://publicintelligence.net/unravelling-trapwire/>

<http://www.nytimes.com/2012/08/14/us/trapwire-antiterrorist-software-leaks-set-off-web-furor.html>

미국, 무인 항공기에 대한 프라이버시 보호 법안 제안

요 약

- 무인항공기 사용 확대의 프라이버시 침해 우려에 따라 미국연방항공국 ‘Modernization and Reform Act’의 개정안 ‘Drone Aircraft Privacy and Transparency Act of 2012’ 발의
- 무인항공기 사용이 프라이버시에 끼치는 영향을 조사하고 프라이버시 보호에 필요한 제반 기준, 절차, 정책 등을 마련

- **(배경)** 무인 항공기 기술 발달과 가격 인하로 무인 항공기 사용이 증가할 것으로 예측되는 가운데 이에 따른 개인의 프라이버시 보호 정책이 미흡함에 따라 관련 법안을 마련하도록 함

※ 미국연방항공국 (FAA, Federal Aviation Administration)에 따르면 2020년까지 비디오 카메라, 무선네트워크 탐지기를 통해 개인정보를 수집 가능한 무인항공기가 30,000대에 이를 것으로 예상

- **(개요)** 2012년 8월 초, 공화당 의원인 Ed Markey는 교통부 장관과 함께 다음 내용이 포함된 ‘Drone Aircraft Privacy and Transparency Act of 2012’을 제안

- 무인항공기가 프라이버시에 끼치는 영향도 조사, 무인항공기 시스템을 국가 항공기 시스템 범위로 통합, 데이터 수집에 필요한 조건 및 절차 마련, 데이터 수집의 최소화 및 모니터링을 위한 정책 마련, 무인항공기 인증 및 면허제도 강화, 무인항공기 사용에 대한 영장의 필요조건 등

- **(주변 동향)** 이와 별도로 국제무인기시스템협회와 국제 경찰청장 협회는 다음과 같은 프라이버시 보호 관련 무인항공기 행동강령 및 가이드라인 제시

※ 국제 경찰청장 협회 (IACP, International Association of Chiefs of Police): 100여 개국 20,000 명 이상의 경찰고위간부들로 구성된 협회로 경찰서비스 향상, 실무상 경험과 정보 등을 공유

※ 국제무인기시스템협회(AUSVSI, Association for Unmanned Vehicle System International): 무인 시스템과 로봇 산업의 홍보와 지원을 목적으로 설립

[무인항공기 행동강령 및 가이드라인]

협회명	제목	프라이버시 보호 관련 내용
국제 경찰청장 협회	무인항공기 사용에 대한 가이드라인	<p>1. 범죄사건·사고 증거 수집을 위해 무인항공기 운영이 필요하고 부득이하게 프라이버시 침해가 예상되는 경우 영장을 발부 받아야 함.</p> <p>2. 범죄 증거, 조사 진행, 훈련 목적, 법에 의해 요구되는 상황을 제외하고 무인항공기를 통해 수집된 이미지 보유 금지</p> <p>3. 법에 의해 면제된 사항이 아니면 수집된 데이터에 대해 국민의 알권리 보장</p>
국제무인기 시스템 협회	무인항공기시스템 사용에 대한 행동강령	<p>1. 개인의 프라이버시를 존중할 것</p> <p>2. 무인항공기 운영에 대한 공공의 우려를 존중할 것</p>

[자료출처]

http://www.gsnmagazine.com/node/27022?c=law_enforcement_first_responders

<http://www.theiacp.org/About/WhatsNew/tabid/459/Default.aspx?id=1848&v=1>

http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf

<http://techdailydose.nationaljournal.com/2012/08/lawmaker-proposes-privacy-prot.php>

<http://www.dronejournalismmlab.org/post/26367021454/auvsi-unmanned-aircraft-system-operations-industry>

<http://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedFiles/AUVSI%20UAS%20Operations%20Code%20of%20Conduct%20-%20Final.pdf>

<http://markey.house.gov/press-release/markey-releases-discussion-draft-drone-privacy-and-transparency-legislation>

미국 FBI, 차세대 얼굴 인식 시스템 도입

요 약

- FBI는 어떠한 상황에서도 92퍼센트의 정확도를 보이는 차세대 얼굴인식시스템을 도입할 것이라 밝힘
- 이에 프라이버시 보호 단체는 본 시스템이 선량한 시민의 생체 인식정보 수집에 따른 또다른 시민 감시 수단에 대한 우려 표명

- **(개요)** 미국 FBI는 Next Generation Identification (NGI) 프로그램의 일환으로 10억 달러를 투자하여 새로운 얼굴인식시스템을 도입할 것을 밝힘
 - 2010년, 파일럿 프로그램 시작하면서 160만 용의자 사진을 대상으로 테스트 해 본 결과 92퍼센트의 정확도를 나타냄
 - 지문, 문신, 손바닥 등의 생체 정보 분석도 가능하며 3-D 기술을 통해 다양한 카메라 각도에서도 높은 얼굴 인식률을 유지
- **(향후 계획)** 미국 전역에 걸친 NGI 운영은 2014년으로 예정, 얼굴인식시스템 사용은 점차 확산되는 추세
 - 미시간 주는 2012년 2월 얼굴인식시스템의 베타버전 운영을 시작했으며 추가적으로 10개 주에서 테스트를 시작했거나 관심을 보이고 있음
- **(기대 효과)** 12,800,000 명의 용의자 이미지가 담긴 데이터베이스를 구축, 도주 중인 용의자 수색을 용이하게 만들 것으로 기대
- **(우려사항)** 용의자 이미지가 SNS, 감시 카메라 등을 통해 수집이 되는 만큼 선량한 시민이 감시의 대상이 될 가능성을 배제할 수 없음
 - 현재는 용의자 사진과 운전면허사진으로 데이터베이스를 구축하고 있으나 FBI에서 사진 수집 범위에 대해 정확히 명시하지 않음

- 얼굴인식시스템을 포함한 NGI가 네트워크상을 통해 개인 생체 정보를 수집한다는 것에 프라이버시 보호 단체는 우려 표명

[자료출처]

<http://vr-zone.com/articles/fbi-invest-1-billion-in-next-gen-face-recognition-system/17149.html>

<http://www.informationweek.com/government/security/fbis-facial-recognition-program-better-s/240007101>

<http://www.slashgear.com/fbi-rolls-out-1-billion-nationwide-facial-recognition-system-10246624/>

FTC, 프라이버시 관련 얼굴인식기술 사용 가이드라인 제시

요 약

- 미국 FTC는 얼굴인식기술 사용 회사 대상 프라이버시 관련 가이드라인 제시
- 가이드라인을 통해 얼굴인식기술을 사용하여 서비스를 제공하는 기업에게 소비자 프라이버시 보호와 함께 지속 성장의 기회 부여

○ FTC는 얼굴인식기술의 발달로 적은 비용으로 좀 더 정확한 이미지 정보 수집이 가능해졌으며 앞으로 얼굴인식기술 사용이 확대될 것이라고 예상

- "Facing Facts - Best Practices for Common Uses of Facial Recognition Technologies" 의 보고서를 통해 얼굴인식기술 사용 가이드라인 제시

○ 보고서의 주요내용

- 2011년 12월, FTC는 Face Facts: A Forum on Facial Recognition Technology 를 통해 논의되었던 얼굴 인식 기술의 발전 내용과 이용 현황 그리고 앞으로 사용될 수 있는 범위에 대해 정리
- 이에 따라 FTC는 얼굴인식기술을 사용하는 회사에게 다음 3가지 사항을 촉구
첫째, 고객의 프라이버시 보호를 유념하여 제품을 개발할 것
둘째, 수집되는 정보에 대해 보안 대책을 마련할 것
셋째, 얼굴 인식 제품과 서비스를 개발할 때 정보의 민감도를 고려할 것

○ (향후 기대) FTC는 얼굴인식기술의 상업적 이용이 아직 초기 단계임을 지적하고 프라이버시 보호기반하에 기술 활용범위 확대 주장

- 추후 얼굴인식을 포함한 생체인식기술을 이용하는 서비스에 대한 모니터링 강화, 산업계와 협력, 이용자 교육 방안 등 구체적인 정책 대안 모색 예정

[자료출처]

<http://www.eweek.com/cloud/ftc-issues-privacy-guidelines-for-facial-recognition-technology/>

<http://www.ftc.gov/os/2012/10/121022facialtechrpt.pdf>

5

글로벌 협력 인식 및 제도간 상호운용성 노력 확대

- ▷ EU, Data Processor 용 BCR(Binding Coportate Rule) 개발
- ▷ 캐나다 - 독일, 데이터 보호 감독기구간 상호 협력 체결
- ▷ 국가별 EU 개인정보보호 Adequacy 평가 진행 경과

EU, Data Processor용 BCR 개발

요 약

- Article 29 Working Party, 데이터수탁처리자(Data Processor)가 개인 정보 국외이전시 준수해야할 Binding Corporate Rules (BCRs) 개발
- 글로벌 아웃소싱의 확대에 따라 국가간 개인정보보호 및 기업들의 계약 절차 간소화 기대

- **(배경)** 국가간 아웃소싱으로 발생하는 개인정보 국외이전의 다양성과 복잡성에 대한 문제점 대두
 - 방대한 고객정보가 이전됨에 따라 보통 수백에서 수천 건의 계약서가 필요하며 각 지역의 데이터 보호 규제기관의 허가를 받아야 하므로 기업들에게 부담으로 작용
 - 데이터처리자 (Data Controller) 뿐만 아니라 데이터를 위탁 받아 처리하는 데이터수탁처리자 (Data Processor)를 위해서도 Binding Corporate Rules의 필요성 대두
- **(주요내용)** Article 29 Working Party는 Data Processor용 Binding Corporate Rules (이후 BCRs) 가이드라인 개발(2013. 1월부터 적용),
 - 기존의 데이터처리자(Data Controller)에게 적용되는 내용에 수탁처리자에게만 해당되는 내용 추가

※ 세부내용은 붙임 참조

- **(기대효과)** Data Processor용 BCRs로 인해 국제적 아웃소싱의 경우 기업들의 계약 절차가 간소화될 것으로 기대됨

[데이터 수탁 처리자의 준수사항]

기존 (데이터 처리자와 공통 적용)	신규(데이터 수탁 처리자에게만 적용)
<ul style="list-style-type: none"> - 관련 구성원과 근로자의 임무 명확화 - 조직개체와 개별 구성원의 연계성 확보 - 유출의 위험이 있는 데이터 관리자와 계약을 맺는 EU 회원국의 의무 부과 - 자체 조사결과 접근 허용, 또는 데이터 보호 책임기관(data protection authorities, DPAs)의 조사 허가할 것 - BCR의 범위에 대한 설명 제공 - BCR이 EU 법과 관련된 개인 데이터 주체에게만 해당하는지, 그 그룹에서 처리되는 모든 개인데이터에 해당되는지 지정 - 투명성, 공정성, 한계의 목적, 데이터 품질, 보안, 정보주체의 권리 포함할 것 	<ul style="list-style-type: none"> - 파산 등으로 데이터처리자가 소멸할 경우, 정보주체의 권리 보호 - 수탁 처리자의 웹사이트에 BCR 공지 - DPA로부터 조사를 받을 의무, 조사된 결과에 대한 조언의 준수 의무 - DPA의 요구사항 또는 정보주체의 불만 사항 등을 포함하여 법률에 제시된 사항과 관련하여 데이터수탁처리자 및 하위수탁처리자에게 데이터관리자를 지원 하는 의무가 포함됨 - 계약 등의 변경으로 인해 처리과정의 변화가 불가피할 경우 데이터처리자에게 사전 공지 의무

[참고기사]

<http://www.huntonprivacyblog.com/2012/06/articles/article-29-working-party-issues-opinion-processor-binding-corporate-rules/>

<http://www.globallawwatch.com/2012/07/analysis-eu-article-29-working-party-requirements-for-processor-binding-corporate-rules-may-ease-international-outsourcings/>

<http://www.huntonprivacyblog.com/2012/12/articles/article-29-working-party-announces-launch-of-binding-corporate-rules-for-processors/#more-3780>

캐나다 - 독일, 데이터 보호를 위한 상호 협력 체결

요 약

- 캐나다-독일의 데이터 보호 위원회는 국민의 디지털 프라이버시 보호를 위해 상호 협력하기로 합의
- 본 합의를 통해 개인정보의 국외이전시 DPA 집행 협력 체계를 굳건히 하고 향후 다른 국가와도 협력의 범위 확대 추진

- **(배경)** 캐나다와 독일은 인터넷을 통한 데이터 전송이 자유로운 환경에서 국민들에게 좀 더 나은 디지털 프라이버시 보호를 제공하기 위해 상호협력하기로 합의
- **(내용)** 양국은 프라이버시 관련 중요한 사건 및 사고 발생 시, 관련 정보를 공유할 것이며 필요할 경우 정부간 협의기반의 조사 등 진행할 예정
 - 독일 데이터 보호 및 정보 자유 위원회의 Peter Schaar는 구글과 페이스북과 같은 회사를 상대하기 위해서는 긴밀한 국제 협력이 필요하다고 밝힘
 - 캐나다 정부는 웹 사용 환경에서 프라이버시 보호 협력의 중요성을 피력하였고 인터넷을 통한 데이터 국외 전송이 자유로운 시대에서 전 세계 데이터 보호 기관의 협력이 절실히 필요하다고 피력
- **(향후 계획)** 두 데이터 보호 기관은 전 세계 관련 기관과의 협력을 확대하기 위해 노력하기로 함

[자료출처]

<http://www.csoonline.com/article/718835/canadian-german-data-protection-watchdogs-join-forces>

국가별 EU 개인정보보호 적합성 평가 진행 경과

요 약

- 개인정보의 국가간 이동이 활발해짐에 따라 EU의 개인정보보호 적합성(Adequacy) 평가제도에 각국의 관심이 확대되고 있음

[2012년 하반기 EU Adequacy Assessment 관련 이슈]

국가	일시	내용
모나코 공국	2012년 7월	Article 29 Working Party가 긍정적인 Opinion을 발표
우루과이	2012년 8월	EC로부터 Adequacy 평가 받음
인도	2012년 9월	EC에게 Adequacy 평가 요청
뉴질랜드	2012년 12월	EC로부터 Adequacy 평가 받음

- (배경) 유럽위원회(European Commission, 이후 EC)는 EU외 제3국의 개인정보보호제도 수준 여부의 적절성(Adequacy)을 위한 평가제도 운영

※ 현재, EU의 adequacy 평가에 대해 적절한 수준이라고 인정받은 나라는 안도라, 아르헨티나, 캐나다의 개인정보보호와 전자문서 법, 페로 제도, 건지, 이스라엘, 저지, 맨섬, 스위스, 미국 상무부(세이프 하버), 우루과이, 뉴질랜드 등 12개국

[적절성 평가제도 운영 단계]

- ① EU와 보다 자유로운 통상을 원하는 국가들은 정해진 양식에 따라 EC에 자국의 개인정보보호제도에 대한 평가 요청
- ② Article 29 Working Party는 관련 조사 후 의견서(Opinion) 제시
- ③ Article 29 Working Party의 의견서를 토대로 EC의 공식적인 결과 발표

[모나코 공국]

- 모나코 공국이 요청한 개인정보보호 adequacy 평가에 대해서 2012년 7월, Article 29 Working Party가 긍정적인 Opinion을 발표
 - 2009년 11월, 모나코 공국이 EC에게 adequacy 평가 요청
 - Article 29 Working Party는 1993년 제정 및 2009년 개정된 모나코의 1993법(Monaco's 1993 Act)에 초점을 맞추어 조사 진행

- 모나코 공국은 Article 29 Working Party의 Opinion에 따라 많이 좌우되는 EC의 마지막 결정을 남겨 놓고 있음

[우루과이]

- 2012년 8월, 4년에 걸친 검토 끝에 우루과이가 EC로부터 개인정보를 적절히 보호하고 있다는 adequacy 평가를 받음
- 2008년, 우루과이가 EC에게 개인정보보호에 대한 adequacy 평가를 요청
- 이에 대해 2010년, Article 29 Working Party가 긍정적인 Opinion을 발표
- 이를 바탕으로 2012년, EC는 우루과이의 개인정보보호가 적절하다는 결론

[인도]

- 2012년 9월, 인도가 EU와의 양자무역협정 중 개인정보보호에 대해 Adequacy 평가를 요청
- 인도는 자국이 요청한 adequacy 평가에 대해 적절하다고 판결되지 않을 경우 양자무역협정을 파기할 것을 주장
- EU는 adequacy 평가를 한다면 이는 양자무역협정과는 별개로 이루어질 것이며, 오랜 시간의 조사 끝에 평가가 이루어진다고 주장함
- ※ 최근 인도에서 일어난 여러 건의 큰 데이터 유출 사건과 관련하여, 인도의 개인정보 보호에 대해 적절하다는 평가가 이루어질지에 대해서는 부정적인 시각들이 있음

[뉴질랜드]

- (개요) 2012년 12월, 뉴질랜드가 EC로부터 개인정보를 적절히 보호하고 있다는 Adequacy 평가를 받음
- 뉴질랜드의 프라이버시 감독국 (Office of the Privacy Commissioner: OPC)은 10여 년간 뉴질랜드 프라이버시 법 1993 (New Zealand's Privacy Act 1993)을 바탕으로 유럽의 adequacy 평가를 받기 위해 노력
- 2011년 4월, Article 29 Working Party가 뉴질랜드 프라이버시 법 1993에 대해 긍정적인 Opinion을 발표
- 이를 바탕으로 2012년, EC는 뉴질랜드의 개인정보보호가 적절하다는 결론

[자료출처]

<http://www.lexology.com/library/detail.aspx?g=bc9794a4-a1ad-4d05-80e0-03d2513d33e1>

<http://www.lexology.com/library/detail.aspx?g=895905a5-1dc8-4516-aa6c-1cae2b7d603c>

<http://www.lexology.com/library/detail.aspx?g=895905a5-1dc8-4516-aa6c-1cae2b7d603c>

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp198_en.pdf

<http://www.scoop.co.nz/stories/PO1212/S00318/european-union-endorses-new-zealand-privacy-act.htm>

<http://www.globalprivacyblog.com/legislative-regulatory-developments/european-working-party-issues-new-zealand-adequacy-opinion/>

6 엔터테인먼트 분야와 어린이 개인정보보호 관심 증가

- ▷ 블리자드 Battle.net, 중국을 제외한 모든 이용자 정보 유출
- ▷ 영국 ICO, 학교 대상 정보보호 가이드 발행
- ▷ 캐나다, 프라이버시 관련 비디오게임 가이드라인 제시
- ▷ 美 FTC, 어린이용 앱 프라이버시 실태조사 실시
- ▷ 美 FTC, 어린이 온라인 프라이버시 보호법 개정

블리자드 Battle.net, 중국을 제외한 모든 이용자 정보 유출

요 약

- 2012년 8월 9일, 블리자드 엔터테인먼트는 Battle.net 이용자 정보의 해킹 사고 발생 성명서 발표
- 이에 Battle.net에서의 사용자 암호 및 본인확인 질문에 대한 답변 변경 권고
 - ※ Battle.net: 전 세계 게임 이용자들이 한자리에 모여 게임을 즐길 수 있는 플랫폼으로 스타크래프트, 디아블로, 월드오브워크래프트 등 블리자드의 인기게임을 하기 위해서는 해당 플랫폼에 접속해야 함

- (사건개요) 2012년 8월 9일, 블리자드 엔터테인먼트에서는 중국을 제외한 모든 이용자의 정보에 대한 해킹사고 발생 성명 발표
 - ‘암호화된 패스워드’, ‘본인확인 질문에 대한 답변’, ‘모바일 인증기’, ‘Battle.net 사용자 이메일 주소’ 등이 해킹됨
 - ※ 2012년 2분기 전 세계 배틀넷 이용자 수는 최대 1690만여 명에 달하며 한국 사용자도 40만 명에 달하는 것으로 알려짐
 - 그러나 신용카드 정보 등 결제정보의 유출 증거는 포착되지 않았다고 설명
- (대응상황) 이에 따라 블리자드 엔터테인먼트는 이번 해킹사고에 다음과 같이 대응
 - 해킹사고에 대응한 소프트웨어 업데이트
 - Battle.net 접속 시, 팝업을 통해 계정암호와 본인확인 질문에 대한 답변을 수정하도록 유도
 - 고객 서비스 센터 직원들에게 게임 플레이어의 신분 확인을 위한 추가조치 통보
 - 이메일 주소의 유출로 인한 이메일 사기 주의 공지
 - Battle.net 접속 암호를 즉시 변경하고 Battle.net 암호와 같거나 비슷한 암호를 이용하는 웹사이트의 암호 또한 변경할 것을 권고

[자료출처]

<http://www.cloudpro.co.uk/cloud-essentials/4317/blizzard-entertainment-confirms-data-breach>

<http://securitywatch.pcmag.com/none/301370-blizzard-confirms-passwords-stolen-in-data-breach>

<http://www.informationweek.com/security/attacks/blizzard-battlenet-security-breached-pas/240005263>

영국 ICO, 학교 대상 개인정보보호 가이드 발행

요 약

- 영국 정보 위원회 (ICO)는 개인정보보호 목적, 데이터 보호 원칙, 관련 기본 교육이 담긴 개인정보보호 가이드를 발행
- 자국의 데이터보호법(Data Protection Act)를 기반으로 13가지 수칙이 포함

○ **(배경)** 영국 정보 위원회 (ICO, Information Commissioner's Office)의 통계에 따르면 학교들이 데이터 보호 의무사항에 대한 준수율이 낮음

※ 400 학교 중 95% 는 개인 정보 활용에 대해 학부모와 학생들에게 정보를 제공

※ 암호 잠금을 설치한 컴퓨터를 보유한 학교 중 30%는 정기적으로 암호를 변경하지 않으며 로그 정보 관리가 미약

※ 학교 중 20%가 학교 이메일 시스템 상 보안에 허점이 있다고 인정

○ **(내용)** 영국 정보 위원회(ICO)는 'Data Protection Act'를 바탕으로 다음 13 가지 항목이 포함된 학교를 위한 개인정보보호 가이드 발행

- **Notification:** 개인 정보 처리에 대한 목적을 명확하게 통보할 것
- **Personal Data:** 데이터 보호 원칙에 맞게 개인 정보를 다룰 것
- **Fair Processing:** 직원과 학생들에게 개인정보 활용 내용에 대해 알릴 것. 오로지 필요한 사람에게만 개인 정보 접근을 허용할 것
- **Security:** 정보를 저장, 사용, 공유 시 기밀성을 유지할 것
- **Disposal:** 기록과 기기를 폐기할 때, 개인 정보가 남아 있지 않도록 할 것
- **Policies:** 직원과 교장이 준수하도록 정보 거버넌스에 대한 명확하고 현실적인 정책과 절차를 마련하고 운영에 대해 모니터링 할 것
- **Subject Access Requests:** 정보 접근 요청에 대해 로그 기록과 모니터링 을 수행할 것
- **Data Sharing:** 정보 공유 허가 여부를 확인하고 공유 시 기밀성을 유지할 것
- **Websites:** 제한 구역에 대한 접근을 통제할 것. 이미지를 포함한 개인 정보가 웹사이트에 공개가 되는 지 여부를 반드시 확인할 것

- **Photographs**: 학교에서 게재 목적으로 사진을 찍은 경우, 공정한 프로세스와 프라이버시 통지에 대한 의도를 함께 공지할 것
- **Processing by Others**: 개인 정보를 제 3 자가 처리 시, 기밀성 보장 여부를 확인할 것
- **Training**: 정보 거버넌스에 대해 직원과 교장을 대상으로 교육을 실시 할 것
- **Freedom of Information (FOI)**: 상담 후, 정보자유법에 따라 어떠한 개인 정보를 제공해야 하는 지 통보할 것

[자료출처]

<http://www.itpro.co.uk/642931/ico-gives-schools-a-lesson-in-data-protection>

http://www.ico.gov.uk/news/latest_news/2012/~media/documents/library/Data_Protection/Research_and_reports/summary_report_dp_guidance_for_schools.ashx

http://www.ico.gov.uk/news/latest_news/2012/~media/documents/library/Data_Protection/Research_and_reports/summary_report_dp_guidance_for_schools.ashx

캐나다, 프라이버시 관련 비디오게임 가이드라인 제시

요 약

- 캐나다 프라이버시 위원회는 쌍방향 비디오게임을 즐기는 모든 연령층에게 프라이버시 관련 가이드라인을 제시
- 위험에 쉽게 노출될 수 있는 어린이 프라이버시 보호를 위해 부모가 함께 게임에 참여할 것을 권고

- **(배경)** 어린이들의 비디오게임 이용이 확대됨에 따라 어린이의 프라이버시 노출 위험이 높아졌으며 게임을 즐기는 모든 연령대에 동일한 위험이 있음을 우려
- **(내용)** 캐나다 프라이버시 위원회는 비디오게임을 할 때 프라이버시 보호를 위해 다음 사항을 유념할 것을 제시함
 - 인터넷을 바탕으로 한 온라인 게임 계정의 경우, 강력한 암호 규칙을 적용할 것 (예. 대소문자, 숫자, 특수문자를 혼합한 암호 권고)
 - 신용카드 정보를 요구하는 계정의 경우, 사용자는 정기적으로 신용카드 사용 내역을 점검해야 하고 이상 발견 시, 즉시 게임회사에 연락토록 할 것
 - 콘솔 혹은 게임이 사용자 프라이버시 통제 기능을 제공할 경우, 사용자가 관련 통제를 유심히 검토하고 선택토록 할 것
 - 게임 계정이 소셜 네트워크 사이트와 연계될 경우, 관련 프라이버시 정책을 검토하고 데이터 수집, 활용, 공유 내용을 확인할 것
 - 게임 참여자 사이에 메시지 교환 (예. 채팅)을 허용하는 환경일 경우, 타인으로부터의 프라이버시 보호 설정을 강화하고 프라이버시 관련 위협을 받을 경우, 즉시 게임 회사에 보고할 것
 - 기타 어린이가 게임 이용시 부모가 함께 참가하도록 권고

[참고기사]

http://www.priv.gc.ca/media/nr-c/2012/nr-c_121105_e.asp

http://www.priv.gc.ca/information/pub/gd_gc_201211_e.asp

http://www.priv.gc.ca/information/pub/gd_gc_201211_e.pdf

미국 FTC, 어린이용 앱 프라이버시 실태 조사 실시

요 약

- 미국 FTC는 2012. 12월, 어린이용 모바일 앱에서 제공하는 프라이버스 관련 정책이 미흡하다고 밝히고, 앱 스토어, 앱 개발자 그리고 앱과 연동하는 제 3자에게 프라이버스 관련 권고안 제시

- (조사보고서 발간) 미국 FTC는 약 400개의 어린이용 모바일 앱의 프라이버시 보호 실태 조사 후 “Mobile Apps for Kids: Disclosures Sill Not Making the Grade”라는 보고서 발간

[주요 조사 결과]

- 조사 대상 400개의 앱 중 20%만이 앱의 프로모션 페이지, 개발자의 웹사이트 혹은 앱 내 프라이버시 관련 공개에 대한 정책 제공함
 - 그러나, 제공된 프라이버시 정책의 내용은 길고 함축적이며 기술적이어서 이해하기가 어려워 정보주체에게 이해를 주는데 한계가 있음을 지적
- 56%의 앱이 모바일 기기 ID를 광고업체, 데이터 분석 회사, 혹은 다른 제3의 회사로 전송하며 5%의 앱이 모바일 기기 ID를 개발자에게 전송
- 3%의 앱만이 위치정보를 개발자, 광고업체에게 전송하고 있으나, 제3자가 어떻게 관련 정보를 이용하는 지는 공개하지 않음

- (권고사항) 이번 보고서를 통해 FTC는 앱 스토어, 개발자, 그리고 앱과 상호작용을 하는 제3자에게 다음 내용을 권고
 - 개인 정보 위협을 최소화하기 위해 ‘privacy-by-design’을 추구할 것
 - 고객에게 관련 데이터 사례에 대해 보다 간단하고 효율적인 선택권 제공할 것
 - 사용자에게 데이터의 수집, 이용, 공유에 대해 명확한 정보를 제공할 것

[참고기사]

<http://www.lexology.com/library/detail.aspx?g=3cefcfdd-32e8-482f-843b-6ffefb7e032b>

<http://www.ftc.gov/opa/2012/12/kidsapp.shtm>

미국 FTC, 어린이 온라인 프라이버시 보호법 개정

요 약

- 미국 연방통상위원회 (FTC)는 모바일 환경 및 신기술에 효율적으로 대응하기 위하여 어린이 온라인 프라이버시 법안 (COPPA, Children's Online Privacy Protection Act 1998) 개정

- (개정 이전 내용) 기존 13세 미만 어린이를 대상으로 한 COPPA의 주요내용은 다음과 같음
 - 어린이 개인 정보 활용에 대한 명백하고 이해하기 쉬운 정책을 공지
 - 어린이로부터 정보 수집 시 부모의 동의 요구
 - 부모에게 어린이 정보 활용 동의 선택권 부여, 어린이 정보의 제3자 제공 금지
 - 부모에게 어린이 개인 정보 검토와 삭제 권한 부여
 - 부모에게 어린이 개인 정보 추가 수집 및 사용을 방지하는 기회 제공
 - 어린이 개인 정보에 대한 기밀성, 보안, 무결성을 유지할 것
- (개정 내용) 제안된 COPPA를 통해 1998년 제정된 COPPA에서 다루지 못했던 최신 정보통신 기술에 대한 프라이버시 위험도를 감소시킬 것임
 - COPPA 규정 적용 범위를 모바일 환경으로 확대
 - 개인정보처리자가 부모 동의를 얻기 위해 간소화되고 자발적이며 투명한 승인 절차 제시 필요
 - 플러그인을 통해 동의없이 개인정보를 수집하는 웹사이트, 모바일 앱 등의 취약점 보완
 - IP 주소 및 모바일 기기 ID 등에서 사용되는 각종 식별자도 본법의 적용대상에 포함
 - 어린이 개인 정보의 사용 요건 및 데이터 보관 및 폐기 절차 강화
- (발효시기) 수정된 COPPA는 2013년 7월 1일부터 발효

[자료출처]

<http://www.mondaq.com/unitedstates/x/201600/Data+Protection+Privacy/FTC+Proposes+Updates+To+Childrens+Online+Privacy+Law>

<http://www.digitaltrends.com/mobile/ftc-updates-childrens-privacy-protection-act/>

<http://www.ftc.gov/opa/2012/12/coppa.shtm>

7

기타

- ▷ 영국 ICO, 공공분야 직원의 개인정보 사용에 대한 안내서 발간
- ▷ 캐나다 IPC, Privacy by Design 안내서 발간
- ▷ OCR, 의료 개인정보 관련 익명화 가이드 발표

영국 ICO, 공공분야 직원의 개인정보 이용에 대한 안내서 발행

요 약

- 영국 정보 위원회인 ICO (Information Commissioner's Office)는 UK Freedom of Information Act 바탕으로 지방자치단체 및 공공기관들의 직원 개인정보 사용에 대한 안내서를 발간
- 이번 지도서를 통해 공공분야 임직원 정보의 사용과 보호 수준을 이해할 수 있는 기회 마련

※ UK Freedom of Information Act: 2000년에 영국에서 수립된 법안으로 공공 기관이 보유하고 있는 정보에 대한 공공의 접근권리에 대해 언급하고 있음

- **(개요)** 외부로부터 공공분야 임직원의 개인정보 요청과 관련하여 ICO는 'Requests for personal data about public authority employees' 지도서를 발간
- **(내용)** 영국의 정보자유법 (Freedom of Information Act)를 근거로 작성되었으며 아래와 같은 내용의 가이드 제시
 - 업무설명(Job description)과 연계된 직원 개인 정보의 범위
 - 공정한 개인정보 공개에 대한 정의
 - 개인정보 공개 거부에 대한 권리
 - 개인정보 공개 시, 필요한 추가 절차 설명 (예. 직원의 동의)
 - 개인 정보 공개 후 절차에 대한 합법성 보장
 - 직원 개인 정보 소유여부에 대해 묵비권 보장
 - 외부가 아닌 내부에서 직원 개인정보 요청시 절차 등

[참고기사]

<http://www.out-law.com/en/articles/2012/august/ico-issues-guidance-on-disclosing-employee-personal-data-under-foi/>

http://www.ico.gov.uk/for_organisations/guidance_index/~/_media/documents/library/Environmental_info_reg/Practical_application/section_40_requests_for_personal_data_about_employees.ashx

캐나다 IPC, Privacy by Design 안내서 발간

요 약

- 캐나다의 온타리오주 정보 프라이버시 감독기구는 프라이버시 안내서 발간하고 “Privacy by Design”을 적용하기 원하는 조직에게 7단계의 단계별 가이드 제시

○ (개요) 2012년 9월 5일, 캐나다의 온타리오 정보 프라이버시 감독원 (Information and Privacy Commissioner of Ontario, 이후, IPC)이 프라이버시 안내서 발간

- 온타리오 주의 프라이버시 감독위원 Cavoukian에 의해 개발된 “Privacy by Design”을 적용하기를 원하는 조직에게 예비 가이드로 지정

※ 원제 : A Policy is Not Enough: It Must be Reflected in Concrete Practices

※ Privacy by Design: 캐나다의 온타리오 정보 프라이버시 감독원 Ann Cavoukian로부터 제시된 개념으로, 프라이버시나 데이터 보호를 기술의 디자인 단계에서부터 적용해야 한다는 의미

○ (주요내용) “Privacy by Design”을 적용하기 원하는 조직들에게 아래의 7단계의 단계별 가이드 제시

- 1단계: 적절한 프라이버시 정책을 실행하고, 개인정보 영향평가 실행 고려
- 2단계: 정책 요구조건과 구체적인 조치항목, 절차, 규제 장치와 연계
- 3단계: 각각의 실행 항목의 이행 가능성 고려
- 4단계: 프라이버시 교육과 인식훈련 프로그램 개발
- 5단계: 프라이버시 관련하여 조언 및 지원자 지정
- 6단계: 감사프로세스 등 신뢰기반의 실행 확인 프로그램 보유
- 7단계: 개인정보 유출에 대비하고 데이터 유출시 대응 규정 수립

[자료출처]

<http://www.mondaq.com/canada/x/195732/data+protection/Beyond+The+Privacy+Policy+New+Guidance>

<http://www.ipc.on.ca/images/Resources/pbd-policy-not-enough.pdf>

OCR, 의료 개인정보 관련 익명화 가이드 발표

요 약

- 2012년 11월, 미국 보건사회복지부 인권사무소(OCR)는 HIPAA에 제시된 프라이버시 규칙을 기반으로 의료 개인정보(PHI)의 익명화 방법 가이드 발표
- HIPAA에서 제시한 두 가지 익명화 방법인 전문가 결정 방법과 세이프하버 방법에 대한 세부내용 제시

- 2012년 11월, 미국 보건사회복지부 인권사무소 (Department of Health and Human Services Office for Civil Rights, 이후 OCR)에서 HIPAA 프라이버시 규칙에 따른 PHI의 익명화 방법 (de-identification)에 대한 가이드 발표

※ HIPAA : 건강보험 양도 및 책임에 관한 법률 (Health Insurance Portability and Accountability Act)

※ PHI : 의료 개인정보 (protected health information)

- HIPAA에서 제시한 두 가지 익명화 방법인 전문가 결정 방법 (Expert Determination Method)과 세이프하버 방법(Safe Harbor Method)에 대해 각각의 가이드 제시

<전문가 결정 방법에 대한 가이드>

- 전문가 결정 방법: 전문가가 식별을 통한 위험을 최소화하기 위해 통계적, 과학적 기법을 적용하는 방법
- 전문가는 특정 전공이나 자격을 필요로 하지 않으며, 다양한 교육과 경험적 배경을 가질 수 있음 (일반적으로 통계, 수학, 과학적 지식 보유)
- OCR은 전문가가 위험을 최소화하기 위한 프로세스 자체를 수립하기 보다는 식별에 의한 위험 수준 정의
- 전문가는 교육, 경험, 익명화 방법과 위험수준평가의 결과들을 문서화

<세이프하버 방법에 대한 가이드>

- 세이프하버 방법 : 명시된 18개의 개인 식별자들을 제거하는 방법
 - 우편번호도 익명화 정보에 포함
 - 환자의 이니셜이나 사회보장번호 뒷 네자리는 PHI를 익명화하는 데에 사용되지 않아야 함
 - 환자의 나이가 89세보다 많을 때에는 ‘90세 이상’ 으로 표시해야 함
 - 익명화 후, 실제 지식(Actual knowledge)이 잔존되어서는 안됨
- ※ 예컨대, 직업이 공개되는 경우, 가족관계가 드러난 경우, 공개된 임상 사건인 경우, 익명화된 PHI를 재조합하여 식별할 수 있는 경우 등

[자료출처]

<http://www.mondaq.com/unitedstates/x/211606/Data+Protection+Privacy/OCR+Issues+Guidance+on+HIPAA+Privacy+Rules+Deidentification+Standard>

<http://www.mondaq.com/unitedstates/x/211026/Healthcare/Office+of+Civil+Rights+Releases+Guidance+on+Deidentification+of+PHI+Under+HIPAA+Privacy+Rule>

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html>

부록

인터넷 세상의 두 빅브라더 : 구글과 페이스북의 개인정보보호 이슈

1. Google

[70여개 서비스의 개인정보 통합관리 정책 추진]

○ (배경) 구글은 2012년 3월, 구글 서비스 내 70 여개 프라이버시 정책 일원화 추진

- 일원화된 정책으로 타겟 광고와 정부기관의 데이터 수집은 용이하나 이용자의 개인정보 자기 결정권은 약화 우려

○ 국가별 대응 현황

구분	내용	조치 내용
유럽 연합 (EU)	Article 29 Working Party	• 통합방침 시행연기 요청 (2.2)
	CNIL (프랑스)	• EU지침 위반 등을 이유로 시행연기 요청 (2.27), 질의서 송부 (3.16) 및 추가질의 (5.22) • 2012년 10월 CNIL는 위법 판결 ※ 사용자 동의 강화, opt-out 도구 중앙집중화 등을 통해 개인정보 제공 선택권 부여, 제한된 목적내 사용토록 조치
일본	총무성 및 경제산업성	• 법령 준수 및 이용자에 대한 고지 누락 등에 대한 개선 권고 (2.29)
캐나다	정 보 보 호 청 (OPC)	• 보유기간 누락, 서비스 간 개인정보 연계 조합 등 여부에 대한 질의서 송부 (2.23)
APPA	기술특별위원회	• 통합 방침 관련 자기정보 통제권에 대한 질의서 송부 (2.28), 구글과 화상회의 (3.21)
홍콩	개인정보보호청 (PCPD)	• 선택권, 개인정보취급방침의 구체성 등에 대해 질의서 송부 (2.28)
호주	개인정보보호청 (OAIC)	• 프라이버시 침해 우려 표명, 조사 착수 발표 (2.3)
미국	전미 검찰총장 협회 (NAAG)	• 우려 표명 서한 발송 (2.22)
	하원	• 사생활 침해 우려 표명 및 질의서 송부 (에너지부, FTC 등)

[스트리트뷰 (Street View), 개인정보 무단 저장]

- **(배경)** 영국 ICO는 2년 전 구글이 스트리트뷰 촬영시 암호화 처리 없이 무단 저장된 개인정보의 완전 삭제명령을 수행하지 않은 문제를 공식 제기
- **(국가별 대응)** 스트리트뷰 잔존 개인정보가 남아있는 국가는 영국, 프랑스, 벨기에를 포함한 10개국, 영국, 프랑스, 호주, 노르웨이는 다음과 같은 대응방안 마련
 - 영국 정보위원회(ICO)는 스트리트뷰 잔존데이터 제출을 명령하고 수사 완료 후 해당 정보의 폐기 방법 및 절차를 전달할 예정
 - 프랑스 정보처리 및 자유에 관한 국가위원회 (CNIL, Commission Nationale de l'informatique et des Libertés)는 구글에 스트리트뷰 잔존 데이터를 제공할 것을 명령
 - 호주 개인정보보호청은 스트리트뷰 데이터를 즉시 삭제하고 제3기관으로부터 삭제 여부를 확인 받아 위원회에 제출하고 다른 디스크에 대한 감사를 실시하여 데이터 잔존 여부를 확인할 것을 명령
 - 노르웨이 개인정보보호 감독기구인 datatilsyne은 불법적으로 개인정보를 취합하고 삭제 명령을 어긴 것에 대해 USD 42,260의 벌금을 부과하고 2012년 10월 1일까지 잔존 데이터 삭제 명령

[자료출처]

<http://www.businessweek.com/news/2012-07-10/google-privacy-report-due-in-september-france-s-cnil-says>

<http://finance.yahoo.com/news/european-ruling-google-privacy-policy-153027087.html>

<http://www.zdnet.com/google-privacy-policy-inquiry-set-for-september-ruling-7000000595/>

<http://euobserver.com/871/115461>

<http://blog.naver.com/oalmephaga?Redirect=Log&logNo=20159819617>

<http://www.itpro.co.uk/641977/ico-confirms-not-all-uk-google-street-view-data-was-destroyed>

<http://www.rte.ie/news/2012/0727/google-retained-private-data-despite-eu-promise.html>

http://www.ico.gov.uk/news/latest_news/2012/statement-ico-response-to-information-received-from-google-27072012.aspx

2. 페이스북

[독일, 페이스북의 얼굴 인식 데이터 삭제 명령]

- (개요) 2012년 8월 15일, 독일의 함부르크 데이터 보호 감독기관은 페이스북의 얼굴 인식 기능(Photo Tag Suggest)에 대한 조사 진행 결정
 - ※ Photo Tag Suggest : 이용자가 페이스북에 올리는 사진을 얼굴 인식 소프트웨어를 통해 분석하여 사진 속 얼굴을 이용자와 자동적으로 매치 시키는 기능
- (내용) 함부르크 감독기관은 페이스북이 얼굴 인식 기능을 이용자들에게 통보하지 않고 사전 동의 없이 도입했으며, 이는 유럽연합회의 법을 위반한 것이라고 밝힘
 - ※ 이와 별도로, 2012년 3월 유럽연합회의 프라이버시 자문 기관인 Article 29 Working Party는 사용자의 명백한 동의 없이 생체 데이터를 수집하는 것은 불법이며 유럽연합회 법을 위반하는 것이라는 성명을 밝힘
- (조치) 독일 데이터 보호 기관은 페이스북에게 독일에서 수집된 얼굴 인식 데이터를 삭제하고 얼굴에 대한 생체 데이터를 수집 시 반드시 사용자의 동의를 받도록 웹사이트를 수정할 것을 명령함

[미국 FTC, 페이스북의 프라이버시 합의서 최종 승인]

- (경과) 2011년 11월, 미국 FTC가 페이스북에 제기한 프라이버시에 관한 혐의에 따라, 미국 FTC와 페이스북이 프라이버시 합의서를 작성
 - 미국 FTC는 페이스북이 개인정보를 공개하지 않기로 하였으나, 지속적으로 개인정보를 외부에 공개하고 있다고 판단하고 혐의를 주장
 - 이에 페이스북은 프라이버시 합의서를 작성함으로써, 앞으로 준수할 사항들을 명시하는 대신 FTC가 제기한 혐의는 무죄로 인정받기로 함
 - FTC는 이 합의내용에 대해 2011년 12월까지 일반의 여론을 수렴
- (내용) 2012년 8월 10일, 미국 FTC는 페이스북과의 프라이버시 합의서의 최종안을 승인
 - 이에 따라, 페이스북은 사용자 정보 공유 시 명확한 공지 필요, 외부 콘텐츠 유통시 사용자의 명시적 동의 필요, 개인정보보호 프로그램 마련·유지 등 준수

- (조치사항) 페이스북은 향후 20년간 격년단위로 정부의 프라이버시 감사 서류 제출 의무 부여, 합의서의 내용을 위반할 시 건별로 하루 16,000달러까지 민사 처벌 대상 조치

[아일랜드 데이터 보호 위원회, 페이스북 감사]

- 아일랜드 데이터 보호 위원회는 페이스북의 법령 위반 여부에 대하여 2회에 걸친 감사 실시 (1차 : 2010. 10~12월, 2차 : 2012. 9월)

○ 1차 감사 결과

- 페이스북의 기능들이 아일랜드 데이터 보호법 1988과 부합하는지 확인
- 페이스북의 안면인식기술, 소셜 플러그인 사용 (‘좋아요’ 버튼), 친구 찾기 기능, 제3자 제공형 어플리케이션 집중적으로 검토
- 다른 이용자와의 정보 공유에 대한 제어 사항과 타겟 광고 등 개인 데이터의 이용범위에 초점을 둠
- 페이스북이 원칙적으로는 아일랜드 데이터 보호법에 부합한다고 결론지었으나 많은 페이스북 기능들에 대해 권고 리스트를 따를 것을 촉구

○ 2차 감사 결과

- 대부분의 권고사항들이 만족스럽게 시행되고 있음
- 프라이버시와 데이터 사용 정책, 광고, 데이터 보유, 쿠키 및 소셜 플러그인, 제3자 제공형 앱, 안면인식/태그 제안 기능, 계정 삭제와 관련하여 방향 제시

- 권고사항 등을 토대로 페이스북은 프라이버시 설정 및 기능 개편

[페이스북의 새로 추가된 프라이버시 설정 및 기능들]

일시	내용
2012년 11월	프라이버시 투어: 페이스북 계정 생성 시 프라이버시 정책에 대한 정보 제공
2012년 11월	각각의 프로필 항목들에 따라 볼 권한 있는 사람 설정 가능
2012년 11월	프라이버시 정책에 대한 투표 실시
2012년 12월	프라이버시 지름길 (Privacy Shortcuts): 프라이버시 정책을 쉽게 수정 가능

[자료출처]

<http://www.4-traders.com/FACEBOOK-INC-10547141/news/Germany-Reopens-Probe-Into-Facebook-s-Face-Recognition-Tool-14463370/>

<http://www.post-gazette.com/stories/business/technology/germany-reopens-facebook-privacy-inquiry-649070/>

<http://www.scmagazine.com.au/News/312466,facebook-facial-recognition-facing-fresh-investigation.aspx>

<http://www.rte.ie/news/2012/0730/data-comm-to-make-facebook-decision-by-october.html>

<http://www.keprtv.com/news/tech/FTC-finalizes-privacy-settlement-with-Facebook-165764096.html>

<http://www.ftc.gov/opa/2012/08/facebook.shtm>

http://www.washingtonpost.com/business/technology/ftc-finalizes-facebook-settlement/2012/08/10/ff620e1c-e2fd-11e1-a25e-15067bb31849_story.html

<http://www.forbes.com/sites/kashmirhill/2012/08/16/germany-is-freaking-out-about-face-books-facial-recognition-feature-again/>

<http://www.itproportal.com/2012/12/13/facebook-once-again-updates-it-privacy-settings/>

2012년 하반기 개인정보보호 해외 정책 동향

“2012년 하반기 개인정보보호 해외 정책 동향”

한국정보화진흥원의 승인 없이 본 내용의 무단전재나 복제를 금합니다.

본 내용에 대한 문의나 제안사항이 있으시면 한국정보화진흥원 개인정보보호 기획부로 연락하여 주시길 바랍니다.

발간일 : 2012. 12. 31

작성 및 편집 : 한국정보화진흥원 개인정보보호기획부

문의 : 김현진 책임연구원 (02-2131-0825) (faerie25@nia.or.kr)