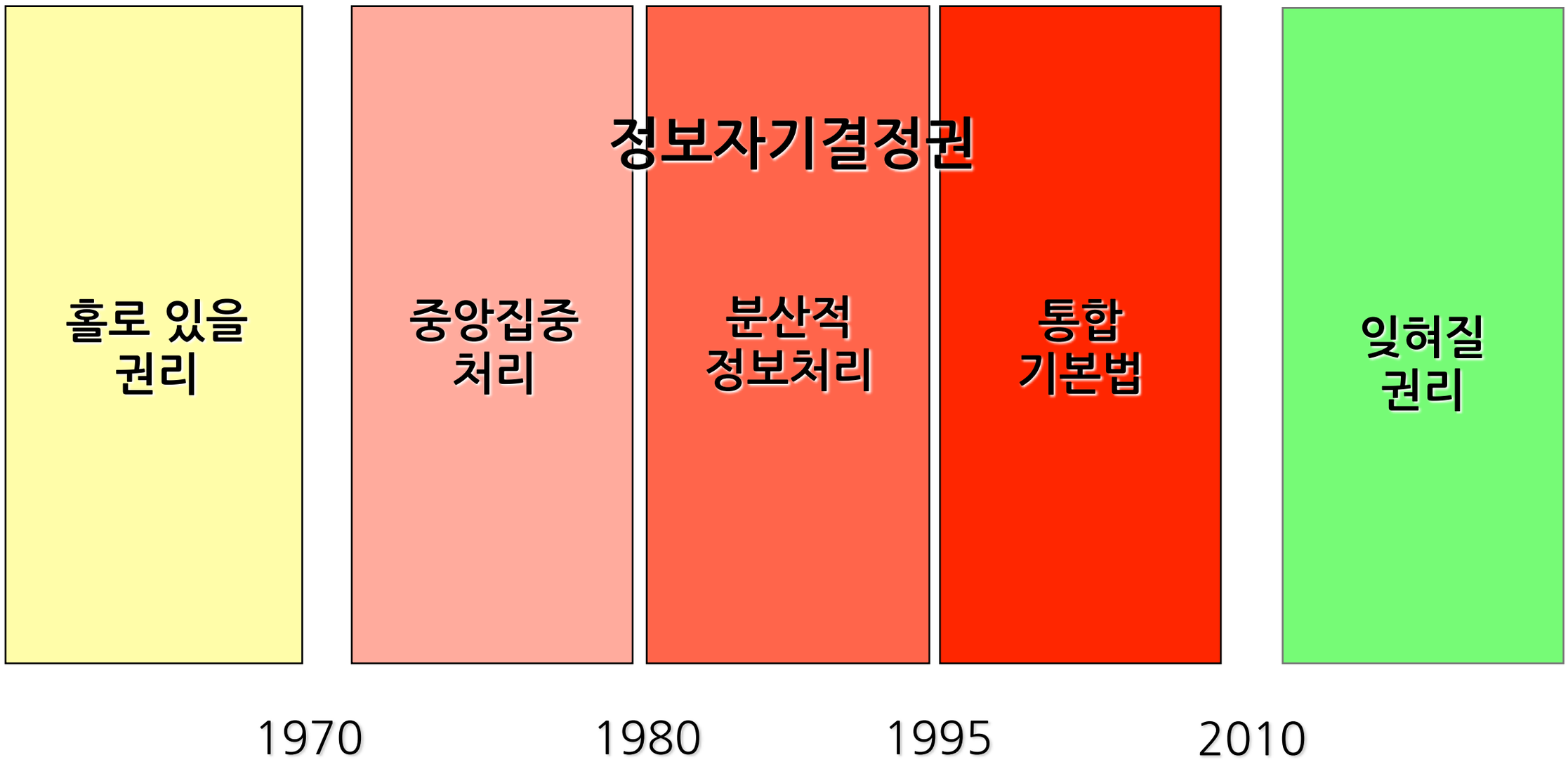
개인정보보호관련 법제의 현황과 이슈

SHIN&KIM | 법무법인 세종

프라이버시 보호의 변천


홀로 있을 권리
중앙집중 처리
정보자기결정권
분산적 정보처리
통합 기본법
잊혀질 권리
1970
1980
1995
2010

개인정보보호법의 법리

SHIN&KIM | 법무법인 세종

개인정보

- 생존하는 개인에 관한 정보
- 개인식별정보
- **간접적인 식별정보도 포함**

개인정보파일

- **개인정보의 집합물**
- **검색의 용이성**
- **체계적으로 배열하거나 구성**

개인정보처리자

- 업무목적
- **개인정보파일 운영**
- 개인정보를 처리

▪ 개인정보처리자 대한 규제법
▪ 이분법적 접근

개인정보보호 법제의 문제점

정비되지 않은 법체계

- 일반법과 특별법의 충돌
- 중복 규제
- 규제기관의 경합

광범위한 규제 범위

- 개인정보의 포괄성
- 광범위한 규제대상
- 민간부문과 공공부문

법리의 경직성

- All or Nothing
- 이익형량의 부재
- 책임의 법정화

인식 부족과 대응 곤란
리스크의 증대

개인정보보호 법제

	공공부문	민간부문
일반법	개인정보보호법	
개별법	•통계법 •공공기관의 정보공개에 관한 법률 •주민등록법 •전자정부법 •교육기본법	•정보통신망 이용촉진 및 정보보호 등에 관한 법률 •신용정보의 이용 및 보호에 관한 법률 •금융지주회사법 •금융실명거래 및 비밀보장에 관한 법률 •전자금융거래법 •통신비밀보호법 •위치정보보호법 •전자서명법 •전자거래기본법 •전자상거래 등에서의 소비자보호에 관한 법률 •의료법 •생명윤리 및 안전에 관한 법률

특별법 우선 원칙의 적용 범위

특별법 우선 원칙의 해석

- 특별법 우선의 원칙은 개인정보보호에 관한 일반법인 「개인정보보호법」과 다른 법률 간의 관계에서도 적용된다고 할 것이고, 다른 법률의 개인정보 제공과 관련된 규정과 「개인정보 보호법」의 규정이 특별법과 일반법 관계에 있는지 여부는 해당 규정의 입법 취지와 내용 등을 종합적으로 검토한 뒤 구체적·개별적으로 판단

구체적 판단

- 다른 법률에서 개인정보를 목적 외로 이용하거나 제3자에게 제공할 수 있도록 규정한 경우 그 내용이 개인정보보호법 제18조 제2항 제2호 외의 다른 항 또는 다른 호의 내용과 충돌하는 것으로 해석되면 개인정보보호법 제18조 제2항, 제4항 제5항이 배제됨

  - ✓ **정보통신망 이용촉진 및 정보보호 등에 관한 법률 제24조의 2 제1항 : 배제 X**
  - ✓ **신용정보의 이용 및 보호에 관한 법률 제32조 제1항, 제2항 및 제4항 : 배제 O**

- 나머지 개인정보보호법의 규정 역시 특별법의 규정과 충돌하는지 여부에 따라 결정

II. 주요 개인정보보호 관련 법률의 개정 현황

개인정보보호법 현황

최근 개정 현황

- (1) 법령에 구체적인 근거, (2) 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요한 경우, (3) 위에 준하여 불가피한 경우로서 안전행정부령으로 정한 경우 외에는 주민번호 수집금지 (2014. 8. 7. 시행)

- 주민번호 암호화 조치 의무, 암호화 대상 및 적용 시기는 대통령령으로 정함 (2016. 1. 1. 시행)

계류 중인 법률안의 주요 내용 - 23개 법안

- 단체소송
- 고유식별정보의 암호화 및 안전성 확보조치 의무화
- 손해배상관련 - 법정손해배상, 피해보상체계 구축
- 유출시 과징금 액수 및 적용대상 확대, 벌금형 강화

정보통신망법 현황

최근 개정 현황

- 14. 5. 4. 위원장 대안 통과
- 개인정보 수집 범위 제한, 누출 등에 대한 통지 및 신고 시한 명시, 파기시 복구불가 조치 및 처벌강화, 법정손해배상액 기준 신설, 정보보호 최고책임자 지정 및 신고 의무

계류 중인 법률안의 주요 내용 - 8개 법안

- 개인정보 보호위원회로 보호 추진체계 일원화
- 피해보상체계 구축 (보험가입 또는 자산예탁)
- 일정규모 이상의 개인정보 저장하는 정보통신서비스 제공자에게 정보보호 관리체계 인증 의무화
- 전반적인 개인정보 보안조치 의무 부여
- 삭제권 강화, 인터넷 몰의 개인정보 침해피해보상 가이드라인,
- 이용자의 사망 이후 개인정보처리방법 지정 및 처리

신용정보법 현황

최근 개정 현황

- 16개 개정안 폐기하고 법안 소위에서 대안 마련하여 정무위 전체회의에 상정(2014. 5. 1.) 했으나 합의 불발
- 2015. 3. 11. 일부개정
  - 개인정보보호법에 대한 특별법임을 명확히 함
  - 정보자기결정권강화 : 수집, 조사 및 처리는 최소 필요한 범위 내로 한정, 개인신용정보의 수집에 관하여 동의 요구
  - 정보주체의 권리보장강화 : 조회권, 통지의무, 징벌적 손해배상 및 법정 손해배상제도 도입
  - 신용정보에 대한 보호절차 강화 : 위탁시 실벽정보 암호화 등 보호조치, 재위탁의 원칙적 금지, 상거래 종료후 5년으로 보유기간 제한
  - 신용조회업 및 신용집중체계 개편 : 신용정보집중기관을 허가제로 변경, 금융기관의 개별신용정보집중기관 폐지, 신용조회회사의 부사업무 제한, 영리목적의 겸업 금지

전부 개정법률안 예고

- 적용대상의 범위 축소
- 신용정보 및 처리개념의 재정립
- 신용정보주체의 권리보장강화
- 신용정보에 대한 보호절차강화

금융지주회사법 현황

최근 개정 현황

- 14. 5. 2. 위원장 대안 통과
- 금융지주회사 내 자회사 등 간 고객의 사전 동의 없이 이루어질 수 있는 정보제공의 목적 한정
- 제공되는 고객정보의 범위, 암호화 및 이용기간 경과 후 삭제 등 금융위원회가 정하는 방법과 절차를 준수
- 제공된 고객정보 이용기간을 법령 준수 등 불가피한 경우를 제외하고 1개월 이내로 제한
- 제공내역을 고객에게 통지하도록 하고, 위반 시 과태료(5천만원이하)

계류 중인 법률안의 주요 내용 - 1개 법안

- 자회사의 고객정보 공유로 인한 손해발생시 금융지주회사의 연대책임

향후 개정 방향

권리구제 및 책임성 강화

- 법정손해배상의 확대. 손해배상책임의 가중, 단체소송확대
- 과징금 기준 상향
- CPO의 임원급 확대, CEO 해임 등 징계권고 대상 확대
- 피해보상체계 구축 (보험가입 또는 자산예탁)

개인정보 최소수집 원칙 강화

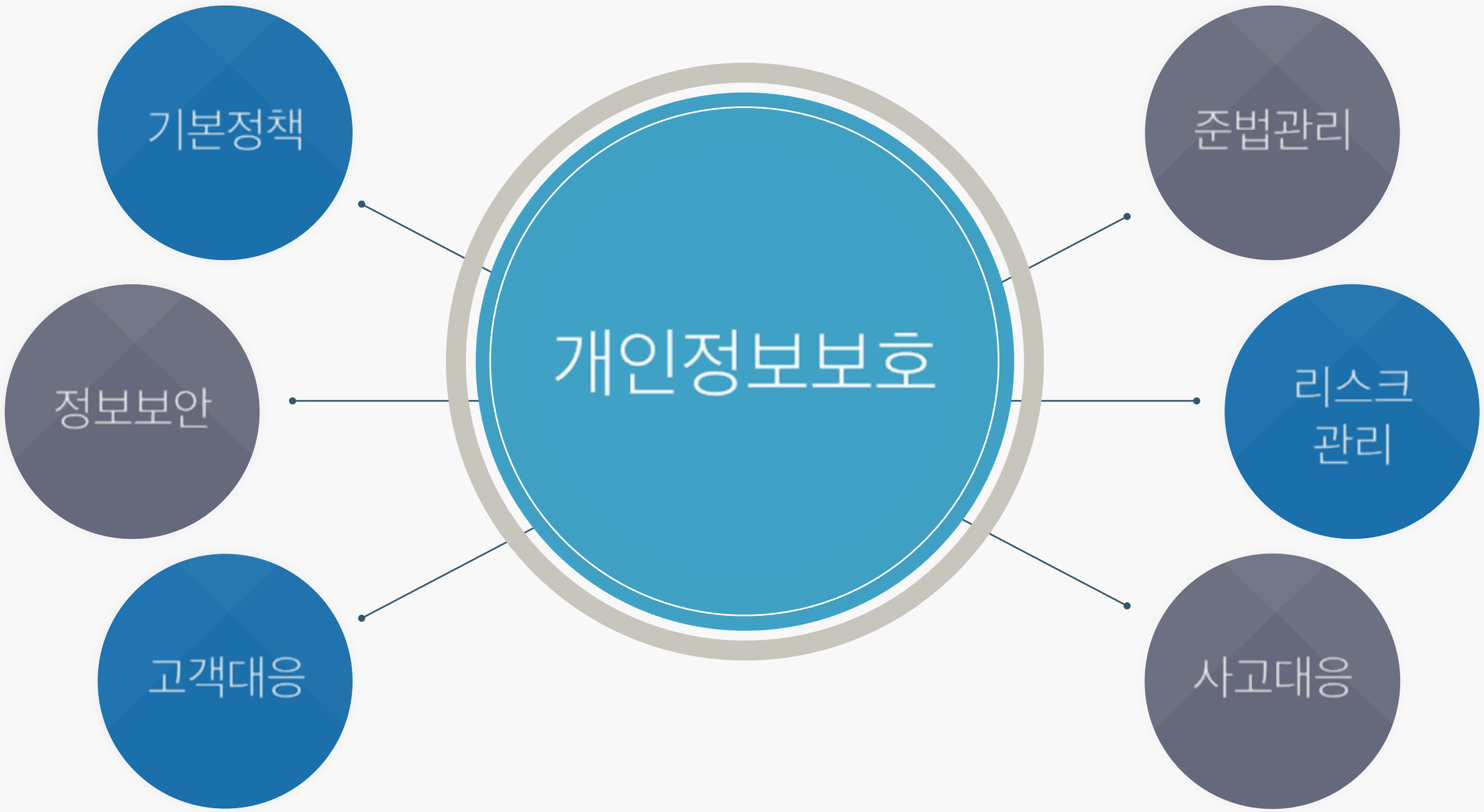
- 고유식별정보 수집 규제, 주민등록번호 관리제도 개선
- 수집 최소화 의무 강화

이용자 편의 확대

- 동의절차 개선
- 삭제요구 절차 간소화
- 권리 확대

개인정보보호 거버넌스

SHIN&KIM | 법무법인 세종



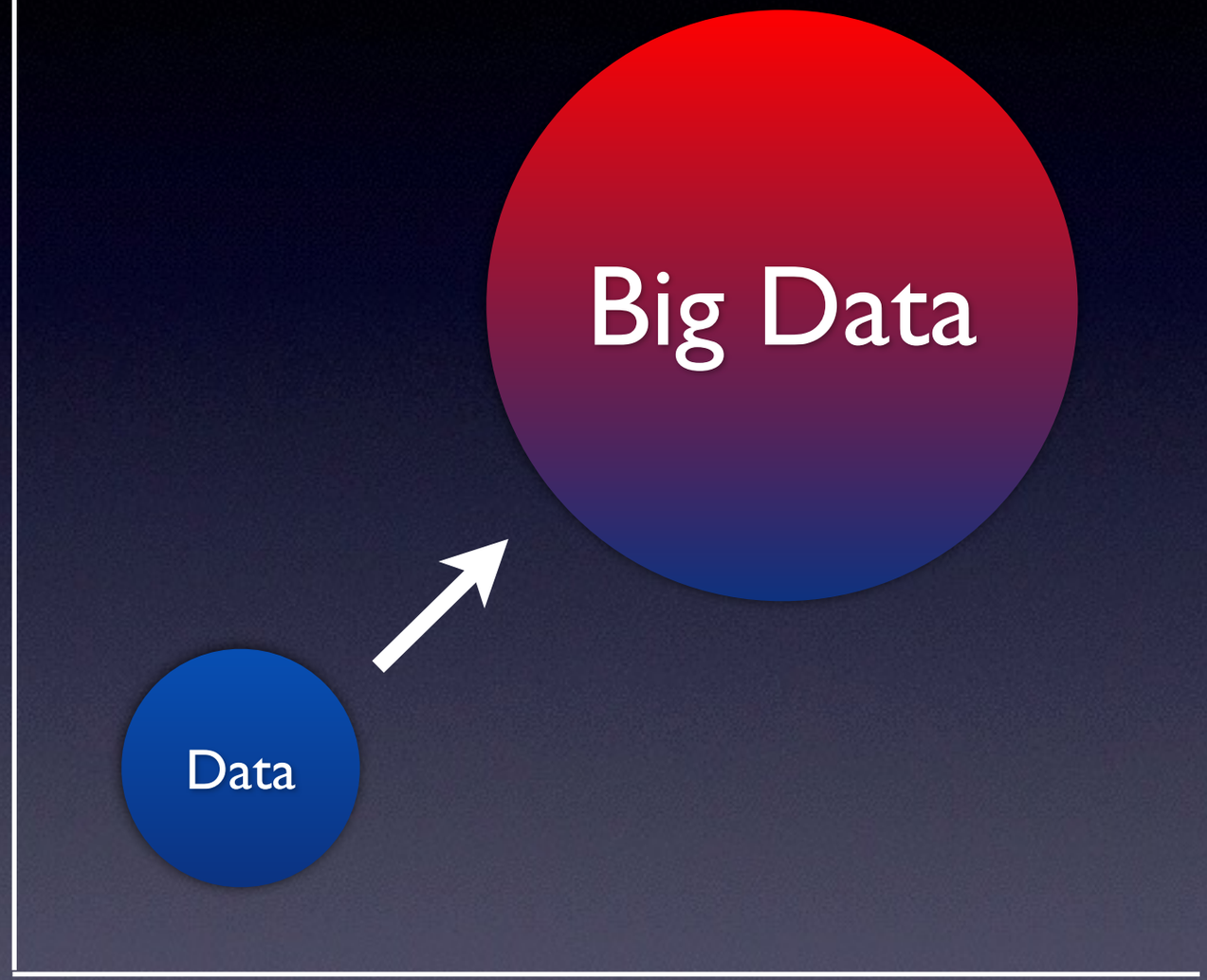
Volume

Variety

Velocity

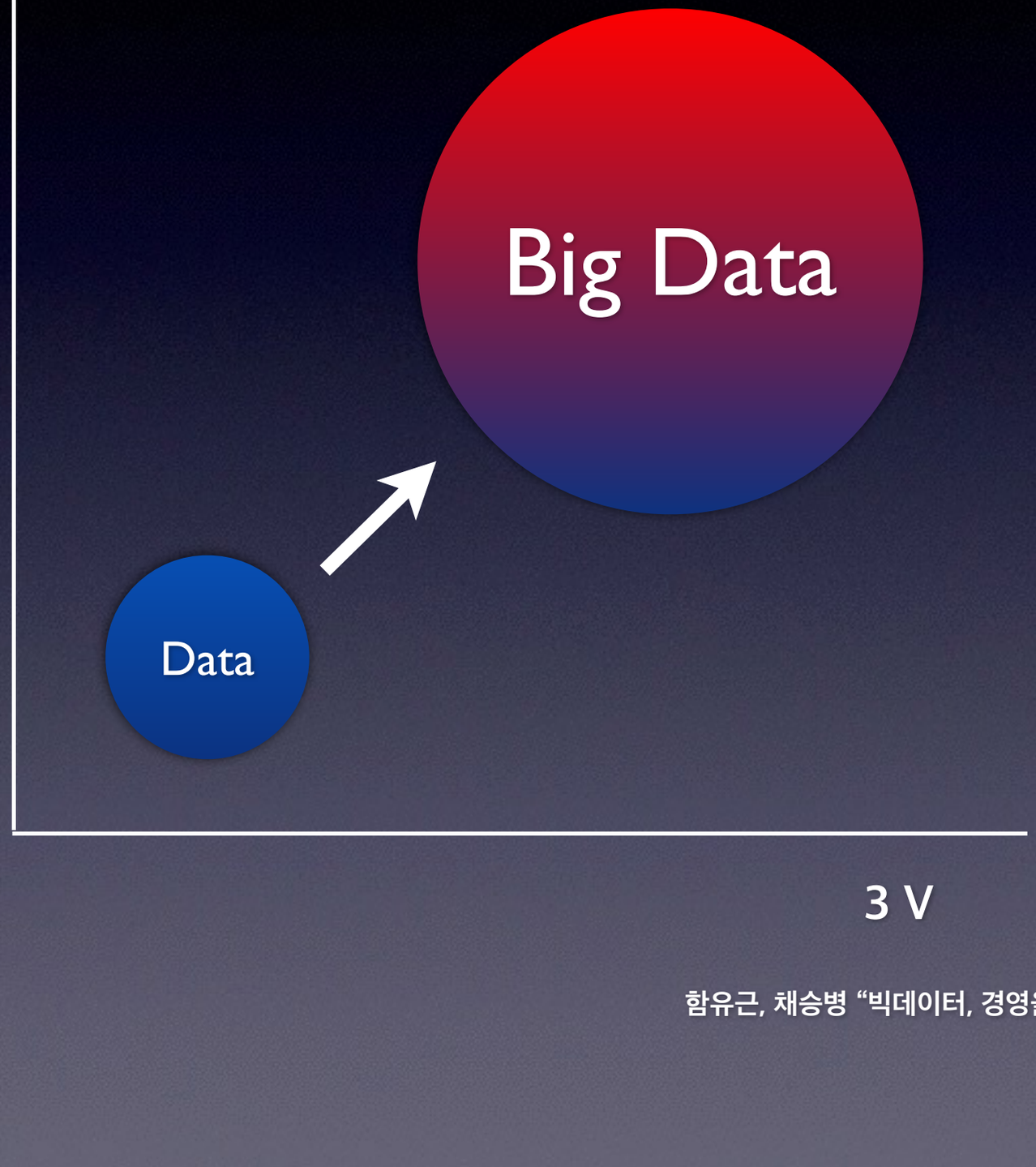
Big Data

데이터의
가치



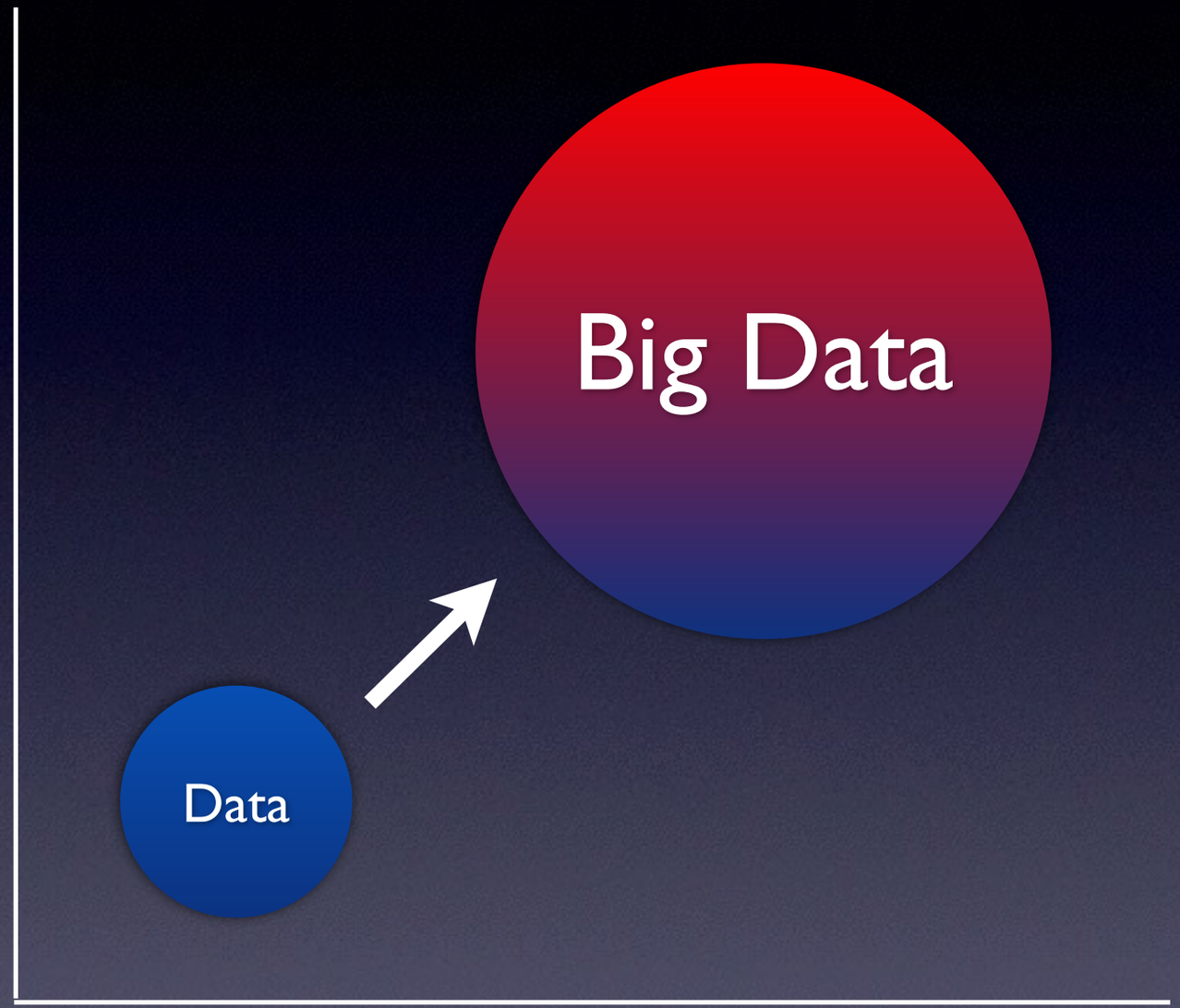
함유근, 채승병 “빅데이터, 경영을 바꾸다” p.41

데이터의
위험성



함유근, 채승병 “빅데이터, 경영을 바꾸다” p.41

데이터의
격차



함유근, 채승병 “빅데이터, 경영을 바꾸다” p.41

비식별화

공개 대상 정보에 개인 식별이 가능한 정보가 포함되어 있는지 여부 등을 사전 필터링

수작업으로 비식별화를 하는 것은 불가능 - 개인정보 스캐닝과 변환 프로그램에 의한 자동처리가 필요

비정형 데이터가 다수를 차지하는 빅데이터의 경우 일정한 규칙에 따라 수집되고 정해진 서식에 따라 관리되는 구조적 데이터에 비해 상대적으로 비식별화 처리가 곤란함

비정형데이터 처리에 있어서는 추가적인 기술적 조치가 필요하나 과도한 필터링의 경우 활용성을 떨어뜨릴 위험성이 있음

데이터 구축 단계부터 XML 등 구조화된 포맷으로 작성하여 제공시에 필요에 따라 개인정보를 포함하고 있는 요소들을 자동으로 삭제 또는 변환 하는 것이 필요.

가명처리
총계 또는 평균값으로 대체
데이터 삭제
범주화
데이터 마스킹

- **식별가능(identifiable)한 정보**

  - Information by which the individual can be identified through simple combination with other information

    EU Directive 95/46/EC on the protection of personal data and GDPR "information relating to an identified or identifiable natural person ; an identifiable person is one who can be identified, directly or indirectly, (by means reasonable likely to be used by the controller or by any other natural or legal person) in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

    Australia, Privacy Act 1988 "personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable"

    Canada, Personal Information Protection and Electronic Documents Act "information about an identifiable individual"

  - Identifiability is the normative concept of rationality, not the technical concept, but tends to be interpreted too broadly, especially in Big Data era.

재식별(Reidentification)의 문제

식별가능정보

자체만으로는 식별되지 않더라도 다른 정보와 쉽게 결합하여 식별되는 정보

직접적인 식별정보 외에 식별가능정보를 개인정보의 개념에서 제외하자는 논의가 있으나 개인정보보호법의 취지에 비추어 그 전부를 개념에서 제외하는 것은 적절치 않음

결국 “쉽게 결합하여 식별”되는지 여부에 따른 판단으로 제한 필요하고, 여기서 쉽게는 물리적, 과학적인 의미가 아닌 합리성에 따른 판단의 의미

결과적으로 식별가능하게 된 정보들을 폭넓게 식별가능정보로 포섭하지 말고 좀더 엄격한 기준에 따라 판단 필요

재식별 정보

비식별정보였으나 다른 정보와 결합됨으로써 결과적으로 식별된 정보

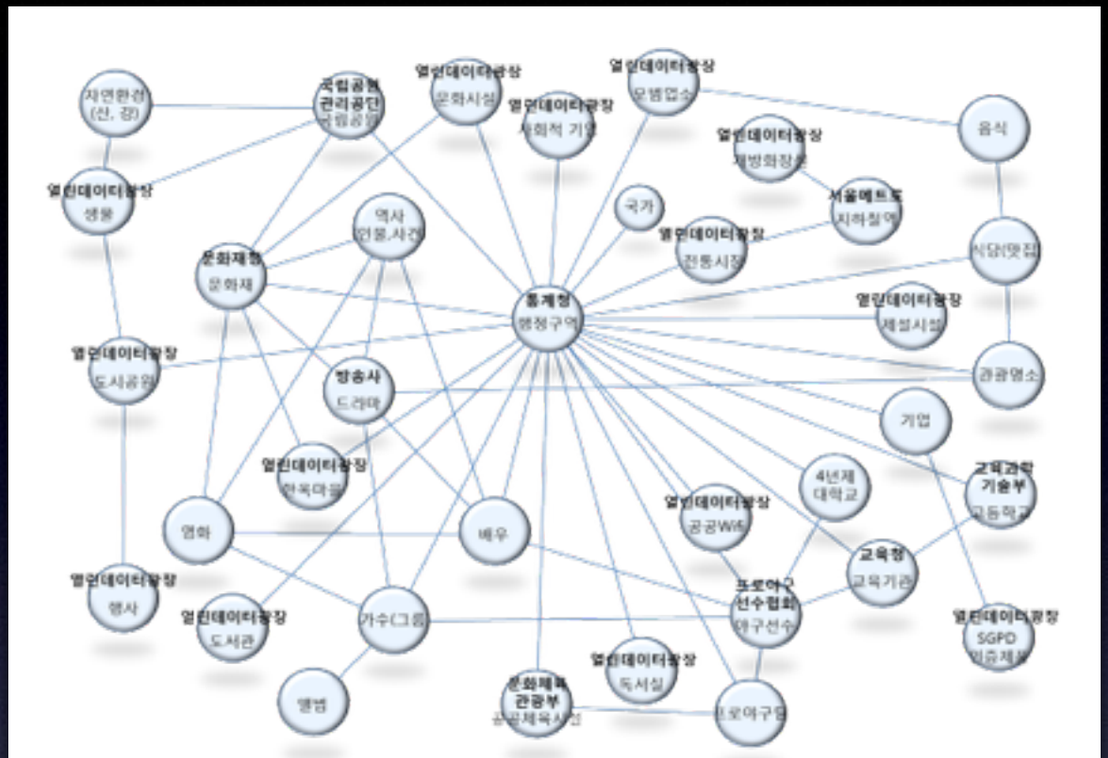
수집·제공단계에서는 “쉽게 결합하여 식별되는” 정보가 아니었으나 다른 정보들과 결합됨으로써 결과적으로 식별되게 된 정보는 (1) opt-out 원칙에 따라 정보주체의 이의가 있으면 다시 비식별조치를 취함으로써 책임을 면하는 방식 또는 (2) 사후 모니터링 의무를 부과하고 그에 대한 고의, 과실 책임을 묻는 방식으로 정보이용자와 정보주체의 이익균형을 도모하는 방안의 고려가 필요

링크드 데이터(Linked Data)와 식별성

링크드 데이터는 웹 상에 존재하는 데이터를 개별 URI로 식별하고, 각 URI에 링크 정보를 부여함으로써 상호 연결된 웹을 지향하는 모형. 컴퓨터가 이해하고 처리할 수 있는 데이터로 된 시맨틱웹의 핵심적 요소

링크드 데이터는 SPARQ 질의를 통해 원하는 방식으로 접근할 수 있고 서로 다른 서버에 한번에 질의가 가능. 또한 해당 객체로 직접 접근할 수 있어 오픈 데이터의 효과적인 사용이 가능. 다른 데이터와도 연계를 시킬 수 있어 활용의 폭이 확대

링크드 데이터는 그 속성상 연결성의 극대화를 가져오므로 정보의 결합으로 인한 식별의 가능성이 커짐. XML과 같이 기계가독형 포맷(machine readable format)의 경우도 같은 맥락.



http://kdata.kr/image/diagram1.png
CCL 적용 제외

이러한 데이터들의 연결성이 식별가능성의 판단에 적극 요소로 고려될 경우 링크드 데이터의 구축이 위출될 우려가 있음 - 사후 모니터링과 opt-out 방식으로 완화할 필요성

- 비식별화의 기술적 한계를 고려한 제안

  - risk based approach

    sensitive information, unique identifying information, user account information vs. other information
    attribution information vs. activity information

  - differential privacy

    emphasis on not whether an individual can be directly associated with a particular revealed value from a data set, but rather the extent to which any revealed value depends on a individual's data

  - Pseudonymous Data in GDPR

    "personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution"

    allowing the controller to process data without consent in order to prevent organization from pursuing a incentive to identify individual strictly to comply with the law

망각에서 기억으로

digital + storage + search + network

web 2.0 service

Social Network Service

Cloud Computing

잊혀질 권리

사실관계 및 경위

- 자신의 부채와 경매에 관한 1998년도 신문기사 및 그 검색 결과의 삭제 구함
- APED는 신문사에 대한 기사 삭제는 기각, 구글 및 구글 스페인에 대한 검색결과 삭제는 인용
- 유럽사법재판소는 구글 및 구글 스페인에 대해 개인정보보호준칙 적용하여 검색 결과 삭제 가능한 것으로 해석

검색서비스에 대한 개인정보보호준칙의 적용여부

- 검색엔진이 정보를 인덱싱, 저장, 분석하고 검색결과를 제공하는 건 개인정보처리(processing)에 해당
- 검색엔진의 운영자는 개인정보처리자(controller)에 해당하여 개인정보보호준칙의 규제대상

검색결과 삭제의 기준

- 정보처리의 적절성(adequate), 관련성(relevant), 비례성(not excessive), 정확성(accurate), 최신성(up to date)의 준수, 수집 및 처리 목적에 비추어 필요한 기간을 초과하여 식별성 있는 상태로 보관되어서는 안됨
- 민감한 사생활에 관한 것으로 16년 경과 - 개인정보보호준칙에 부합하지 않는 데이터 처리이므로 삭제, 차단청구 인정
- 검색서비스 업체의 기술적, 경제적 부담 증가, 공중의 접근권, 표현의 자유 등 다른 법익과의 비교형량 문제

EU에서의 잊혀질 권리 (right to be forgotten)

유럽과 미국의 대조

유럽 : 인격권 보호의 관점
미디어로부터의 보호
인간의 존엄성 최우선

미국 : 재산권 보호의 관점
공권력으로부터의 보호
표현의 자유 최우선

미국 정보산업에 대한 견제

국가중요정보의 보호
국부유출방지
데이터주권론

잊혀질 권리는 적법 정보에 대한 정보주체의 권리
기존의 삭제권의 확대
예외사유의 입증책임 문제
대상정보의 범위의 모호성

IoT의 의미

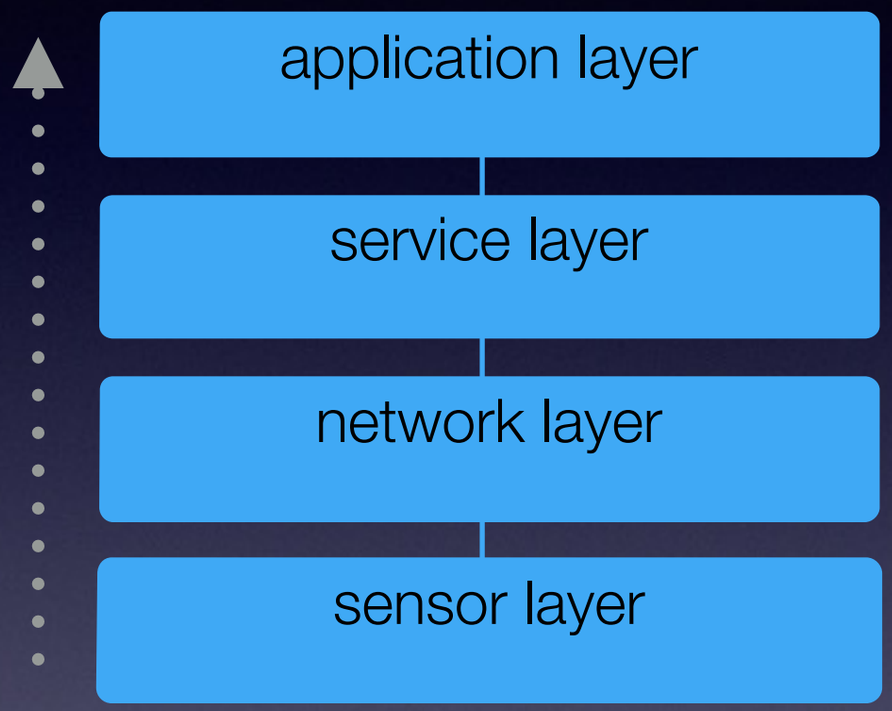
USN(ubiquitous sensor network)
M2M(machine to machine)
IoT(internet of things)
IoE(internet of everything)

“ talking to the analog world around us in a digital way with all the benefits of digital communication”
-Daniel Kellmereit, ‘the Silence Intelligence’

상호 작용하는 사물들의 네트워크

→ 정보의 공유 & 결정과 조치

IoT의 구조 및 기술



자산관리 건강 에너지 환경
교통 생산관리 smart home

결제 시스템 보안
데이타 분석 플랫폼 데이타 관리

bluetoothe zigbee UMTS
LTE Wifi NFC

RFID Photo-electric 온도
Barcode Gyroscope GPS

data transport
data analysis
data acqusition

miniatuarization
affordability
de-wireization

파생되는 쟁점들

- 규제와 기준 (Regualtion and Standard)
- 실업 (Job Losses)
- 책임 소재(Tort Liability)
- 데이터 소유(Data Ownership)
- 개인정보(Personal Information Protection)
- 보안 (Cyber Security)
- 망 관리, 망 중립성(Net Neutrality)

Cyber Security

http://www.computerweekly.com/news/2240224012/IoT-smart-light-bulbs-get-security-update

데이터 보안
시스템 침입 및 조작
테러, 범죄의 가능성

취약 부분

- IoT 디바이스
- IoT 디바이스 간 네트워킹
- 데이터 보관

표준의 부족

개인정보

https://flic.kr/p/84VZAr
https://creativecommons.org/licenses/by-sa/2.0/

목적 외 사용 문제

개인정보

최소수집의 원칙 보장 문제

정보주체의 통제권 보장 문제
- 자동처리
- 개인정보정책 확인 불가
- 처리과정에 대한 정보부족
- informed consent 곤란

데이타 분석에 대한 문제
- 빅 데이타
- 프로파일링
  - *ICDPPC*의 프로파일링 결의안 *(*알고리듬의 검증 및 감독*)*

개인정보

CCTV

지능형 영상인식기술
지능형 통합관제 서비스

개인정보보호법 제25조

1. 법령
2. 범죄의 예방 및 수사
3. 시설안전 및 화재예방
4. 교통단속
5. 교통정보의 수집, 분석 및 제공

목적 외 조작, 영상정보의 목적 외 이용 금지

개인정보

목적 외 이용 및 제공의 제한

수집 단계에서의 방어수단 부존재

추상적인 목적 하에 자유로운 설치 허용
개인정보 수집 회피는 사실상 불가능

이용 단계에서의 엄격한 규제 필요

수집목적 범위 내에서의 이용과 제공
명시적 수권규정에 의해서만 목적외 사용 허용

개인정보

관련 사례

버스 내부에 설치된 CCTV
교통사고 증거수집 및 범죄예방 목적으로 설치

징계나 근무평정 목적의 사용 여부

개인정보보호위원회의 의결

> “버스회사가 교통사고 증거수집 및 범죄예방의 목적으로 버스안에 설치한 CCTV는 해당 목적에 맞게 사용하여야 한다. 다만, 법령에서 구체적으로 허용하고 있는 경우는 예외로 한다. 수집된 녹화물을 CCTV 설치 목적과 직접 관계없는 운전기사의 징계 또는 근무평정의 증거자료로 사용하는 것은 허용되지 않는다. 다만, 개인정보보호법 제18조 제2항의 예외 사유에 해당하는 경우에는 그 범위 내에서 허용될 수 있다”

개인정보

통신비밀보호법

한정된 대상과 엄격한 법적 절차 하에서만 통신 및 대화의 비밀과 자유에 대한 제한

불법검열이나 불법감청에 의한 내용의 증거능력부정

적법한 통신제한조치의 내용도 그 목적이 된 동법 제5조 제1항의 특정범죄나 관련 범죄의 수사, 소추, 그 범죄 예방, 그 범죄로 인한 징계절차, 통신의 당사자가 제기하는 손해배상소송, 기타 다른 법률의 규정에 의한 경우등으로 한정하여 증거능력 인정

개인정보

Privacy by Design

7대 기본원칙

- 사후 대응이 아니라 사전 대비, 문제점을 고치는 것이 아니라 예방 *Proactive /Preventative*
- 프라이버시 보호를 기본 설정값으로 *By Default*
- 계획에 포함된 프라이버시 *Embedded*
- 포괄적 기능성 보장 - 상호대체가 아닌 상호보완 *Positive Sum*
- 시작에서 끝까지 보안 - 전체 수명주기의 보호 *Lifecycle Protection*
- 가시성과 투명성 - 항상 공개 *Visibility/Transparency*
- 개인의 프라이버시 존중 - 사용자 중심의 설계와 운영 *Respect the Users*

SHIN&KIM | 법무법인 세종

감사합니다

윤종수 파트너변호사

T. 02 316 4040
F. 02 756 6226
E. jsyoon@shinkim.com

서울시 중구 퇴계로 100 스테이트타워 남산 8층 (우)100-052 I TEL: +82 2 316 4114 I FAX: +82 2 756 6226

www.shinkim.com