Privacy Laws in Germany and Europe

Johannes Waldmann, HTWK Leipzig

19. Oktober 2015

Privacy: Definitions

- “data protection” (Datenschutz)
  protecting the rights of invdividuals
  with respect to processing information (data)
  that is, or can be, associated to their person.
  (processing by individuals, companies, state institutions)
- “data security” (Datensicherheit)
  technical methods, tools and procedures that are helpful to achieve this goal (and others)

this talk: focus on the legal aspects,
in Germany and European Union

Privacy: Definitions

- “data protection” (Datenschutz)
  protecting the rights of invdividuals
  with respect to processing information (data)
  that is, or can be, associated to their person.
  (processing by individuals, companies, state institutions)
- “data security” (Datensicherheit)
  technical methods, tools and procedures that are helpful to achieve this goal (and others)

this talk: focus on the legal aspects,
in Germany and European Union

Privacy: Definitions

- “data protection” (Datenschutz)
  protecting the rights of invdividuals
  with respect to processing information (data)
  that is, or can be, associated to their person.
  (processing by individuals, companies, state institutions)
- “data security” (Datensicherheit)
  technical methods, tools and procedures that are helpful to achieve this goal (and others)

this talk: focus on the legal aspects,
in Germany and European Union

Privacy: Definitions

- “data protection” (Datenschutz)
  protecting the rights of invdividuals
  with respect to processing information (data)
  that is, or can be, associated to their person.
  (processing by individuals, companies, state institutions)
- “data security” (Datensicherheit)
  technical methods, tools and procedures that are helpful to achieve this goal (and others)

this talk: focus on the legal aspects,
in Germany and European Union

Disclaimer: I Am Not A Lawyer,

and this is not legal advice.

What you read here, (hopefully)

- gives the correct general idea,

but certainly

- is not complete
- is simplified.

who am I (for this talk)?

- I am not speaking in my capacity as HTWK's privacy officer (Datenschutzbeauftragter).
- this is an academic lecture (in my capacity as professor of computer science).

Disclaimer: I Am Not A Lawyer,

and this is not legal advice.

What you read here, (hopefully)

- gives the correct general idea,

but certainly

- is not complete
- is simplified.

who am I (for this talk)?

- I am not speaking in my capacity as HTWK's privacy officer (Datenschutzbeauftragter).
- this is an academic lecture (in my capacity as professor of computer science).

Processing of personal information

. . . is necessary for society to function

- state: processes personal data for
  e.g., elections, taxation, law enforcement,
  . . . (discuss: infrastructure?)
- companies: process personal data . . .
  - of employees, e.g., wages
  - of customers, e.g., banks, insurance, car rental, . . . (discuss: supermarket?)
  - of unrelated, unsuspecting third persons, e.g., for market research

. . . can be mis-used, threat of mis-use already restricts person's freedom (e.g., of speech)

. . . invites mis-use by third parties (criminals)

Processing of personal information

. . . is necessary for society to function

- state: processes personal data for
  e.g., elections, taxation, law enforcement,
  . . . (discuss: infrastructure?)
- companies: process personal data . . .
  - of employees, e.g., wages,
  - of customers, e.g. banks, insurance, car rental, . . . (discuss: supermarket?)
  - of unrelated, unsuspecting third persons, e.g., for market research

. . . can be mis-used, threat of mis-use already restricts person's freedom (e.g., of speech)

. . . invites mis-use by third parties (criminals)

Processing of personal information

. . . is necessary for society to function

- state: processes personal data for
  e.g., elections, taxation, law enforcement,
  . . . (discuss: infrastructure?)
- companies: process personal data . . .
  - of employees, e.g., wages,
  - of customers, e.g. banks, insurance, car rental, . . . (discuss: supermarket?)
  - of unrelated, unsuspecting third persons, e.g., for market research

. . . can be mis-used, threat of mis-use already restricts person's freedom (e.g., of speech)

. . . invites mis-use by third parties (criminals)

Processing of personal information

. . . is necessary for society to function

- state: processes personal data for
  e.g., elections, taxation, law enforcement,
  . . . (discuss: infrastructure?)
- companies: process personal data . . .
  - of employees, e.g., wages,
  - of customers, e.g. banks, insurance, car rental, . . . (discuss: supermarket?)
  - of unrelated, unsuspecting third persons, e.g., for market research

. . . can be mis-used, threat of mis-use already restricts person's freedom (e.g., of speech)

. . . invites mis-use by third parties (criminals)

Processing of personal information

. . . is necessary for society to function

- state: processes personal data for
  e.g., elections, taxation, law enforcement,
  . . . (discuss: infrastructure?)
- companies: process personal data . . .
  - of employees, e.g., wages,
  - of customers, e.g. banks, insurance, car rental, . . . (discuss: supermarket?)
  - of unrelated, unsuspecting third persons, e.g., for market research

. . . can be mis-used, threat of mis-use already restricts person's freedom (e.g., of speech)

. . . invites mis-use by third parties (criminals)

Processing of personal information

. . . is necessary for society to function

- state: processes personal data for
  e.g., elections, taxation, law enforcement,
  . . . (discuss: infrastructure?)
- companies: process personal data . . .
  - of employees, e.g., wages,
  - of customers, e.g. banks, insurance, car rental, . . . (discuss: supermarket?)
  - of unrelated, unsuspecting third persons, e.g., for market research

. . . can be mis-used, threat of mis-use already restricts person's freedom (e.g., of speech)

. . . invites mis-use by third parties (criminals)

Processing of personal information

. . . is necessary for society to function

- state: processes personal data for
  e.g., elections, taxation, law enforcement,
  . . . (discuss: infrastructure?)
- companies: process personal data . . .
  - of employees, e.g., wages,
  - of customers, e.g. banks, insurance, car rental, . . . (discuss: supermarket?)
  - of unrelated, unsuspecting third persons, e.g., for market research

. . . can be mis-used, threat of mis-use already restricts person's freedom (e.g., of speech)

. . . invites mis-use by third parties (criminals)

Processing of personal information

. . . is necessary for society to function

- state: processes personal data for
  e.g., elections, taxation, law enforcement,
  . . . (discuss: infrastructure?)
- companies: process personal data . . .
  - of employees, e.g., wages,
  - of customers, e.g. banks, insurance, car rental, . . . (discuss: supermarket?)
  - of unrelated, unsuspecting third persons, e.g., for market research

. . . can be mis-used, threat of mis-use already restricts person's freedom (e.g., of speech)

. . . invites mis-use by third parties (criminals)

Privacy Laws: Historic precedents

German/European privacy laws influenced by:

- confidentiality for certain professions
  medical doctors, attorneys, priests, journalists
- German national census (Volkszählung) 1983 declared unlawful by highest German court because it violates basic human right of *informational self-determination* (informationelle Selbstbestimmung)
- East German (1949–1989) citizens under constant surveillance by state secret service, using collected (and fabricated) data for accusations, imprisonment, expatriation

Privacy Laws: Historic precedents

German/European privacy laws influenced by:

- confidentiality for certain professions
  medical doctors, attorneys, priests, journalists
- German national census (Volkszählung) 1983 declared unlawful by highest German court because it violates basic human right of *informational self-determination* (informationelle Selbstbestimmung)
- East German (1949–1989) citizens under constant surveillance by state secret service, using collected (and fabricated) data for accusations, imprisonment, expatriation

Privacy Laws: Historic precedents

German/European privacy laws influenced by:

- confidentiality for certain professions
  medical doctors, attorneys, priests, journalists
- German national census (Volkszählung) 1983 declared unlawful by highest German court because it violates basic human right of *informational self-determination* (informationelle Selbstbestimmung)
- East German (1949–1989) citizens under constant surveillance by state secret service, using collected (and fabricated) data for accusations, imprisonment, expatriation

Law Making in Germany

fundamental procedure

- citizens elect parlamentarians
- parlament (discussed and) passes laws
- president signs and formally announces laws

on several levels

- state (e.g., city of Leipzig belongs to state of Saxony, capital Dresden)
- federation (Federal Republic of Germany, capital Berlin)
- European union (parlament in Strasbourg, Bruselles, Luxembourg)

Law Making in Germany

fundamental procedure

- citizens elect parlamentarians
- parlament (discussed and) passes laws
- president signs and formally announces laws

on several levels

- state (e.g., city of Leipzig belongs to state of Saxony, capital Dresden)
- federation (Federal Republic of Germany, capital Berlin)
- European union (parlament in Strasbourg, Bruselles, Luxembourg)

Law Making in Germany

fundamental procedure

- citizens elect parlamentarians
- parlament (discussed and) passes laws
- president signs and formally announces laws

on several levels

- state (e.g., city of Leipzig belongs to state of Saxony, capital Dresden)
- federation (Federal Republic of Germany, capital Berlin)
- European union (parlament in Strasbourg, Bruselles, Luxembourg)

Laws for Privacy

- state: Sächsisches Datenschutzgesetz
  processing of personal data by state institutions
  e.g., of student data, by universities
- federation: Bundesdatanschutzgesetz
  . . . by private and commercial entities
  discuss: location of online service providers
- Europe
  . . . 1995: data protection directive (directive)
  . . . 2018 ?: data prot. regulation (law without ratification)

Laws for Privacy

- state: Sächsisches Datenschutzgesetz
  processing of personal data by state institutions
  e.g., of student data, by universities
- federation: Bundesdatanschutzgesetz
  . . . by private and commercial entities
  discuss: location of online service providers
- Europe
  - 1995: data protection directive (directive)
  - 2018 ?: data prot. regulation (law enforcement)

Laws for Privacy

- state: Sächsisches Datenschutzgesetz
  processing of personal data by state institutions
  e.g., of student data, by universities
- federation: Bundesdatanschutzgesetz
  . . . by private and commercial entities
  discuss: location of online service providers
- Europe
  - 1995: data protection directive (Richtlinie)
  - 2018 ?: data prot. regulation (Verordnung)

Laws for Privacy

- state: Sächsisches Datenschutzgesetz
  processing of personal data by state institutions
  e.g., of student data, by universities
- federation: Bundesdatanschutzgesetz
  . . . by private and commercial entities
  discuss: location of online service providers
- Europe
  - 1995: data protection directive (Richtlinie)
  - 2018 ?: data prot. regulation (Verordnung)

Laws for Privacy

- state: Sächsisches Datenschutzgesetz
  processing of personal data by state institutions
  e.g., of student data, by universities
- federation: Bundesdatanschutzgesetz
  . . . by private and commercial entities
  discuss: location of online service providers
- Europe
  - 1995: data protection directive (Richtlinie)
  - 2018 ?: data prot. regulation (Verordnung)

Processing by State Institutions

- processing of personal data is *prohibited*
- *unless* explicitly allowed *by law* (or regulation):
  - Hochschulgesetz (Higher Education Law) (§5) tasks of universities (§14) what personal data can be processed
  - university regulations for library, computers, ...
- if allowed, then only to the *minimal necessary* extent for realizing *the specific task*
- each person has the right to
  - know all their data that is being processed
  - have data corrected, deleted, ...

Processing by State Institutions

- processing of personal data is *prohibited*
- *unless* explicitly allowed *by law* (or regulation):
  - Hochschulgesetz (Higher Education Law) (§5) tasks of universities (§14) what personal data can be processed
  - university regulations for library, computers,
- if allowed, then only to the *minimal necessary* extent for realizing *the specific task*
- each person has the right to
  - know all their data that is being processed
  - have data amended, deleted or blocked

Processing by State Institutions

- processing of personal data is *prohibited*
- *unless* explicitly allowed *by law* (or regulation):
  - Hochschulgesetz (Higher Education Law) (§5) tasks of universities (§14) what personal data can be processed
    - university regulations for library, computers,
- if allowed, then only to the *minimal necessary* extent for realizing *the specific task*
- each person has the right to
  - know all their data that is being processed
  - have data amended, deleted or blocked

Processing by State Institutions

- processing of personal data is *prohibited*
- *unless* explicitly allowed *by law* (or regulation):
  - Hochschulgesetz (Higher Education Law) (§5) tasks of universities (§14) what personal data can be processed
  - university regulations for library, computers,
- if allowed, then only to the *minimal necessary* extent for realizing *the specific task*
- each person has the right to
  - know all their data that is being processed
  - have data amended, blocked or deleted

Processing by State Institutions

- processing of personal data is *prohibited*
- *unless* explicitly allowed *by law* (or regulation):
  - Hochschulgesetz (Higher Education Law) (§5) tasks of universities (§14) what personal data can be processed
  - university regulations for library, computers,
- if allowed, then only to the *minimal necessary* extent for realizing *the specific task*
- each person has the right to
  - know all their data that is being processed
  - have data amended, that is not true

Processing by State Institutions

- processing of personal data is *prohibited*
- *unless* explicitly allowed *by law* (or regulation):
  - Hochschulgesetz (Higher Education Law) (§5) tasks of universities (§14) what personal data can be processed
  - university regulations for library, computers,
- if allowed, then only to the *minimal necessary* extent for realizing *the specific task*
- each person has the right to
  - know all their data that is being processed,
  - have data corrected, deleted, blocked

Processing by State Institutions

- processing of personal data is *prohibited*
- *unless* explicitly allowed *by law* (or regulation):
  - Hochschulgesetz (Higher Education Law) (§5) tasks of universities (§14) what personal data can be processed
  - university regulations for library, computers,
- if allowed, then only to the *minimal necessary* extent for realizing *the specific task*
- each person has the right to
  - know all their data that is being processed,
  - have data corrected, deleted, blocked

Processing by State Institutions

- processing of personal data is *prohibited*
- *unless* explicitly allowed *by law* (or regulation):
  - Hochschulgesetz (Higher Education Law) (§5) tasks of universities (§14) what personal data can be processed
  - university regulations for library, computers,
- if allowed, then only to the *minimal necessary* extent for realizing *the specific task*
- each person has the right to
  - know all their data that is being processed,
  - have data corrected, deleted, blocked

Privacy Officer

each state institution has a Privacy Officer (Datenschutzbeauftragter). Tasks:

- know the laws,
  help (both sides) in applying them
- check personal data processing
  (while it is being done, and before)
- help in resolving disputes
  (e.g., between student and administrative office)

this officer operates *independently*
(can inspect all details, rector cannot give orders)

Privacy Officer

each state institution has a Privacy Officer (Datenschutzbeauftragter). Tasks:

- know the laws,
  help (both sides) in applying them
- check personal data processing
  (while it is being done, and before)
- help in resolving disputes
  (e.g., between student and administrative office)

this officer operates *independently*
(can inspect all details, rector cannot give orders)

Privacy Officer

each state institution has a Privacy Officer (Datenschutzbeauftragter). Tasks:

- know the laws,
  help (both sides) in applying them
- check personal data processing
  (while it is being done, and before)
- help in resolving disputes
  (e.g., between student and administrative office)

this officer operates *independently*
(can inspect all details, rector cannot give orders)

Public and Private Sector

laws for processing of personal data by public (state) institutions are very strict,

- purpose is to protect the citizen
  - because the state is much more powerful
  - and the citizen has no choice

laws for processing of personal data by private (commercial) entities are somewhat different:

- people are free to enter/negotiate contracts
- there is a choice (of service providers, . . .)

still there are rules, to protect customers' interests (cf. merchants, air transportation)

Public and Private Sector

laws for processing of personal data by public (state) institutions are very strict,

- purpose is to protect the citizen
- because the state is much more powerful
- and the citizen has no choice

laws for processing of personal data by private (commercial) entities are somewhat different:

- people are free to enter/negotiate contracts
- there is a choice (of service providers, . . .)

still there are rules, to protect customers' interests (cf. merchants, air transportation)

Public and Private Sector

laws for processing of personal data by public (state) institutions are very strict,

- purpose is to protect the citizen
- because the state is much more powerful
- and the citizen has no choice

laws for processing of personal data by private (commercial) entities are somewhat different:

- people are free to enter/negotiate contracts
- there is a choice (of service providers, . . .)

still there are rules, to protect customers' interests (cf. merchants, air transportation)

Public and Private Sector

laws for processing of personal data by public (state) institutions are very strict,

- purpose is to protect the citizen
- because the state is much more powerful
- and the citizen has no choice

laws for processing of personal data by private (commercial) entities are somewhat different:

- people are free to enter/negotiate contracts
- there is a choice (of service providers, . . .)

still there are rules, to protect customers' interests (cf. merchants, air transportation)

Public and Private Sector

laws for processing of personal data by public (state) institutions are very strict,

- purpose is to protect the citizen
- because the state is much more powerful
- and the citizen has no choice

laws for processing of personal data by private (commercial) entities are somewhat different:

- people are free to enter/negotiate contracts
- there is a choice (of service providers, . . .)

still there are rules, to protect customers' interests (cf. merchants, air transportation)

Processing by Companies

- for many businesses, processing of personal data of their customers is central and obvious task (finance, insurance, . . .)
- for others, this is *central but non-obvious*,
  - often deliberately obfuscated
  - not restricted to customers,
    extended to users of web sites
  - even of unrelated web sites
- often with companies that offer “free” services
  if the service is free,
  it is the client that is being sold.

Processing by Companies

- for many businesses, processing of personal data of their customers is central and obvious task (finance, insurance, . . .)
- for others, this is *central but non-obvious*,
  - often deliberatly obfuscated
  - not restricted to customers,
    extended to users of web sites
  - even of unrelated web sites
- often with companies that offer “free” services

  if the service is free,
  it is the client that is being sold.

Processing by Companies

- for many businesses, processing of personal data of their customers is central and obvious task (finance, insurance, . . .)
- for others, this is *central but non-obvious*,
  - often deliberatly obfuscated
  - not restricted to customers,
    extended to users of web sites
  - even of unrelated web sites
- often with companies that offer “free” services
  if the service is free,
  it is the client that is being sold.

Processing by Companies

- for many businesses, processing of personal data of their customers is central and obvious task (finance, insurance, . . .)
- for others, this is *central but non-obvious*,
  - often deliberatly obfuscated
  - not restricted to customers, extended to users of web sites
  - even of unrelated web sites
- often with companies that offer “free” services

if the service is free,
it is the client that is being sold.

Processing by Companies

- for many businesses, processing of personal data of their customers is central and obvious task (finance, insurance, . . .)
- for others, this is *central but non-obvious*,
  - often deliberatly obfuscated
  - not restricted to customers, extended to users of web sites
  - even of unrelated web sites
- often with companies that offer “free” services

if the service is free,
it is the client that is being sold.

Processing by Companies

- for many businesses, processing of personal data of their customers is central and obvious task (finance, insurance, . . .)
- for others, this is *central but non-obvious*,
  - often deliberatly obfuscated
  - not restricted to customers, extended to users of web sites
  - even of unrelated web sites
- often with companies that offer “free” services

if the service is free,
it is the client that is being sold.

“Free service” business model

- the business of commercial search engine providers, “social” network providers, . . . is *selling advertising space to their customers*
- so, in order to increase their profit, they want to
  1. attract more targets for advertising (users)
  2. know the (shopping) preferences of their targets better
- they (hope to) achieve this by
  1. cool services, changes of terms, increase user interface upgrades after (free) registration
  2. aggregating and evaluating personal data

“Free service” business model

- the business of commercial search engine providers, “social” network providers, . . . is *selling advertising space to their customers*
- so, in order to increase their profit, they want to
  1. attract *more* targets for advertising (“users”)
  2. know the (shopping) preferences of their targets better
- they (hope to) achieve this by
  1. real services, chances of “exclusive” user upgrades after (free) registration
  2. aggregating and evaluating personal data

“Free service” business model

- the business of commercial search engine providers, “social” network providers, . . . is *selling advertising space to their customers*
- so, in order to increase their profit, they want to
  1. attract *more* targets for advertising (“users”)
  2. know the (shopping) preferences of their targets better
- they (hope to) achieve this by
  1. paid services, charges for “premium” users, upgrades after (free) registration
  2. aggregating and evaluating personal data

"Free service" business model

- the business of commercial search engine providers, "social" network providers, . . . is *selling advertising space to their customers*
- so, in order to increase their profit, they want to
  1. attract *more* targets for advertising ("users")
  2. know the (shopping) preferences of their targets better
- they (hope to) achieve this by
  1. cool services, claims of "everyone else uses it", upgrades after (free) registration
  2. aggregating and evaluating personal data

“Free service” business model

- the business of commercial search engine providers, “social” network providers, . . . is *selling advertising space to their customers*
- so, in order to increase their profit, they want to
  1. attract *more* targets for advertising (“users”)
  2. know the (shopping) preferences of their targets better
- they (hope to) achieve this by
  1. cool services, claims of “everyone else uses it”, upgrades after (free) registration
  2. aggregating and evaluating personal data

“Free service” business model

- the business of commercial search engine providers, “social” network providers, . . . is *selling advertising space to their customers*
- so, in order to increase their profit, they want to
  1. attract *more* targets for advertising (“users”)
  2. know the (shopping) preferences of their targets better
- they (hope to) achieve this by
  1. cool services, claims of “everyone else uses it”, upgrades after (free) registration
  2. aggregating and evaluating personal data

“Free service” business model

- the business of commercial search engine providers, “social” network providers, . . . is *selling advertising space to their customers*
- so, in order to increase their profit, they want to
  1. attract *more* targets for advertising (“users”)
  2. know the (shopping) preferences of their targets better
- they (hope to) achieve this by
  1. cool services, claims of “everyone else uses it”, upgrades after (free) registration
  2. aggregating and evaluating personal data

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for "storing user preferences")
- third-party cookies (for continuous tracking)
- e.g., `google-analytics.com/ga.js`
- URL shortening services
- DNS resolver service

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for “storing user preferences”)
- third-party cookies (for continuous tracking)
- `ajax.googleapis.com/jquery.min.js`
- URL shortening services
- DNS resolver service

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion
  (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for “storing user preferences”)
- third-party cookies (for continuous tracking)
- `ajax.googleapis.com/jquery.min.js`
- URL shortening services
- DNS resolver service

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion
  (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for “storing user preferences”)
- third-party cookies (for continuous tracking)
- `ajax.googleapis.com/jquery.min.js`
- URL shortening services
- DNS resolver service

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion
  (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for “storing user preferences”)
- third-party cookies (for continuous tracking)
- `ajax.googleapis.com/jquery.min.js`
- URL shortening services
- DNS resolver service

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion
  (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for “storing user preferences”)
- third-party cookies (for continuous tracking)
- `ajax.googleapis.com/jquery.min.js`
- URL shortening services
- DNS resolver service

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion
  (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for “storing user preferences”)
- third-party cookies (for continuous tracking)
- `ajax.googleapis.com/jquery.min.js`
- URL shortening services
- DNS resolver service

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion
  (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for “storing user preferences”)
- third-party cookies (for continuous tracking)
- `ajax.googleapis.com/jquery.min.js`
- URL shortening services
- DNS resolver service

Some Ways To Collect Your Data

obvious: store your web site, photos, calendar, e-mail

not that obvious (but if you think for a moment . . .)

- online translation services
- real-time auto-completion
  (typing speed and spelling errors)
- browser identification (including OS name)
- cookies (for “storing user preferences”)
- third-party cookies (for continuous tracking)
- `ajax.googleapis.com/jquery.min.js`
- URL shortening services
- DNS resolver service

Key Points of Forthcoming EU Policy

`http://ec.europa.eu/justice/data-protection/reform/`

- right to “be forgotten”
- whenever consent is required, it must be given explicitly, rather than be assumed
- right of data portability (change of provider)
- applicable also for processing outside EU

Is this “killing internet economy”?

- hopefully, it kills the worst instances of it
- it improves the market (creates jobs) for privacy-sensitive service providers

Key Points of Forthcoming EU Policy

`http://ec.europa.eu/justice/data-protection/reform/`

- right to “be forgotten”
- whenever consent is required, it must be given explicitly, rather than be assumed
- right of data portability (change of provider)
- applicable also for processing outside EU

Is this “killing internet economy”?

- hopefully, it kills the worst instances of it
- it improves the market (creates jobs) for privacy-sensitive service providers

Key Points of Forthcoming EU Policy

`http://ec.europa.eu/justice/data-protection/reform/`

- right to “be forgotten”
- whenever consent is required, it must be given explicitly, rather than be assumed
- right of data portability (change of provider)
- applicable also for processing outside EU

Is this “killing internet economy”?

- hopefully, it kills the worst instances of it
- it improves the market (creates jobs) for privacy-sensitive service providers

Key Points of Forthcoming EU Policy

`http://ec.europa.eu/justice/data-protection/reform/`

- right to “be forgotten”
- whenever consent is required, it must be given explicitly, rather than be assumed
- right of data portability (change of provider)
- applicable also for processing outside EU

Is this “killing internet economy”?

- hopefully, it kills the worst instances of it
- it improves the market (creates jobs) for privacy-sensitive service providers

What Can You Do Now?

as individuals

- know how much of your (and your friends') personal data you are paying for "free" services
- think of the long-term implications (your employment, credit approval, health insurance)
- know your citizen rights, and exercise them

as (future) IT professionals: (all of the above and) learn and apply technologies for privacy:

- design systems that use personal data sparingly
- secure communication on insecure channels
- secure storage on untrusted servers

What Can You Do Now?

as individuals

- know how much of your (and your friends') personal data you are paying for "free" services
- think of the long-term implications (your employment, credit approval, health insurance)
- know your citizen rights, and exercise them

as (future) IT professionals: (all of the above and) learn and apply technologies for privacy:

- design systems that use personal data sparingly
- secure communication on insecure channels
- secure storage on untrusted servers

What Can You Do Now?

as individuals

- know how much of your (and your friends') personal data you are paying for "free" services
- think of the long-term implications (your employment, credit approval, health insurance)
- know your citizen rights, and exercise them

as (future) IT professionals: (all of the above and) learn and apply technologies for privacy:

- design systems that use personal data sparingly
- secure communication on insecure channels
- secure storage on untrusted servers

What Can You Do Now?

as individuals

- know how much of your (and your friends') personal data you are paying for "free" services
- think of the long-term implications (your employment, credit approval, health insurance)
- know your citizen rights, and exercise them

as (future) IT professionals: (all of the above and) learn and apply technologies for privacy:

- design systems that use personal data sparingly
- secure communication on insecure channels
- secure storage on untrusted servers

What Can You Do Now?

as individuals

- know how much of your (and your friends') personal data you are paying for "free" services
- think of the long-term implications (your employment, credit approval, health insurance)
- know your citizen rights, and exercise them

as (future) IT professionals: (all of the above and) learn and apply technologies for privacy:

- design systems that use personal data sparingly
- secure communication on insecure channels
- secure storage on untrusted servers

Security in Untrusted Environments

the message should be encrypted,
but the (decryption) key cannot be transported safely.
solutions for secure end-to-end encryption:

- public (encryption) key
  - decryption key remains private
  - RSA (relies on hardness of factoring)
  - used in PGP (email end-to-end encryption) and for authenticity (signature) checking
- construction of shared (session) keys
  - Diffie-Hellman (. . . of discrete logarithm)
  - used in HTTPS, SSH, TLS

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi of university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi of university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi at university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi at university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi at university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi of university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi of university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi of university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Separate Service from Authentication

- service provider (SP) delegates authentication to identity provider (IdP),
- SP does not receive/store password information
- example: Shibboleth protocol, example:
  - SP: shared distance learning service for universities in Saxony
  - IdP: student's home university
- example: eduroam (guest WiFi access)
  - SP: WiFi of university hosting a conference
  - IdP: participant's home university
- SP can provide anonymous services (IdP does not tell authenticated user's identity to SP)

Experiments: Your Data on the Web

- find out what information your browser sends:
  in a shell, run `nc -l -p 9999` (keep running);
  in browser, open `http://localhost:9999/`
- find out to what additional web sites your data gets sent (Firefox → Tools → Web Developer → Network, ctrl-shift-Q)
- confirm that your browsers sends keystrokes as you type search terms (same method)
- view your cross-site tracking cookies with Lightbeam (previously: Collusion) Firefox plugin
- compare to data in the "EU cookie sweep" (find the official report, using a safe search engine)

Experiments: Your Data on the Web

- find out what information your browser sends: in a shell, run `nc -l -p 9999` (keep running); in browser, open `http://localhost:9999/`
- find out to what additional web sites your data gets sent (Firefox → Tools → Web Developer → Network, ctrl-shift-Q)
- confirm that your browsers sends keystrokes as you type search terms (same method)
- view your cross-site tracking cookies with Lightbeam (previously: Collusion) Firefox plugin
- compare to data in the "EU cookie sweep" (find the official report, using a safe search engine)

Experiments: Your Data on the Web

- find out what information your browser sends: in a shell, run `nc -l -p 9999` (keep running); in browser, open `http://localhost:9999/`
- find out to what additional web sites your data gets sent (Firefox → Tools → Web Developer → Network, ctrl-shift-Q)
- confirm that your browsers sends keystrokes as you type search terms (same method)
- view your cross-site tracking cookies with Lightbeam (previously: Collusion) Firefox plugin
- compare to data in the "EU cookie sweep" (find the official report, using a safe search engine)

Experiments: Your Data on the Web

- find out what information your browser sends: in a shell, run `nc -l -p 9999` (keep running); in browser, open `http://localhost:9999/`
- find out to what additional web sites your data gets sent (Firefox → Tools → Web Developer → Network, ctrl-shift-Q)
- confirm that your browsers sends keystrokes as you type search terms (same method)
- view your cross-site tracking cookies with Lightbeam (previously: Collusion) Firefox plugin
- compare to data in the "EU cookie sweep" (find the official report, using a safe search engine)

Experiments: Your Data on the Web

- find out what information your browser sends: in a shell, run `nc -l -p 9999` (keep running); in browser, open `http://localhost:9999/`
- find out to what additional web sites your data gets sent (Firefox → Tools → Web Developer → Network, ctrl-shift-Q)
- confirm that your browsers sends keystrokes as you type search terms (same method)
- view your cross-site tracking cookies with Lightbeam (previously: Collusion) Firefox plugin
- compare to data in the “EU cookie sweep” (find the official report, using a safe search engine)

Experiment: break RSA encryption

- private key: (p, q) both prime
- public key: (e, m) where $m = pq$ and $\gcd(e, \phi(m)) = 1$ with $\phi(m) = (p-1)(q-1)$
- encrpytion of cleartext t is $t^e \bmod m$
- decryption of ciphertext c is $c^A \bmod m$ where A, B such that $A \cdot e + B \cdot \phi(m) = 1$, compute A, B by extended Euclidean algorithm
- proof: $Ae \equiv 1 \bmod \phi(m)$, thus $(c^e)^A \equiv c^1$ using Fermat's "little" theorem $c^{\phi(m)} \equiv 1 \bmod m$
- Ex: $p = 3, q = 11,\ m = 33, e = 3, \phi(m) = 20,$ $A = 7, B = -1, 7 \overset{enc}{\to} 7^3 \equiv 13 \overset{dec}{\to} 13^7 \equiv 7.$

Experiment: break RSA encryption

- private key: (p, q) both prime
- public key: (e, m) where $m = pq$ and $\gcd(e, \phi(m)) = 1$ with $\phi(m) = (p-1)(q-1)$
- encrpytion of cleartext t is $t^e \bmod m$
- decryption of ciphertext c is $c^A \bmod m$ where A, B such that $A \cdot e + B \cdot \phi(m) = 1$, compute A, B by extended Euclidean algorithm
- proof: $Ae \equiv 1 \bmod \phi(m)$, thus $(c^e)^A \equiv c^1$ using Fermat's "little" theorem $c^{\phi(m)} \equiv 1 \bmod m$
- Ex: $p = 3, q = 11,\ m = 33, e = 3, \phi(m) = 20,$ $A = 7, B = -1, 7 \overset{enc}{\to} 7^3 \equiv 13 \overset{dec}{\to} 13^7 \equiv 7.$

Experiment: break RSA encryption

- private key: (p, q) both prime
- public key: (e, m) where $m = pq$ and $\gcd(e, \phi(m)) = 1$ with $\phi(m) = (p-1)(q-1)$
- encrpytion of cleartext t is $t^e \bmod m$
- decryption of ciphertext c is $c^A \bmod m$ where A, B such that $A \cdot e + B \cdot \phi(m) = 1$, compute A, B by extended Euclidean algorithm
- proof: $Ae \equiv 1 \bmod \phi(m)$, thus $(c^e)^A \equiv c^1$ using Fermat's "little" theorem $c^{\phi(m)} \equiv 1 \bmod m$
- Ex: $p = 3, q = 11,\ m = 33, e = 3, \phi(m) = 20,$ $A = 7, B = -1, 7 \overset{enc}{\to} 7^3 \equiv 13 \overset{dec}{\to} 13^7 \equiv 7.$

Experiment: break RSA encryption

- private key: (p, q) both prime
- public key: (e, m) where $m = pq$ and $\gcd(e, \phi(m)) = 1$ with $\phi(m) = (p-1)(q-1)$
- encrpytion of cleartext t is $t^e \bmod m$
- decryption of ciphertext c is $c^A \bmod m$ where A, B such that $A \cdot e + B \cdot \phi(m) = 1$, compute A, B by extended Euclidean algorithm
- proof: $Ae \equiv 1 \bmod \phi(m)$, thus $(c^e)^A \equiv c^1$ using Fermat's "little" theorem $c^{\phi(m)} \equiv 1 \bmod m$
- Ex: $p = 3, q = 11,\ m = 33, e = 3, \phi(m) = 20,$ $A = 7, B = -1, 7 \overset{enc}{\to} 7^3 \equiv 13 \overset{dec}{\to} 13^7 \equiv 7.$

Experiment: break RSA encryption

- private key: (p, q) both prime
- public key: (e, m) where $m = pq$ and $\gcd(e, \phi(m)) = 1$ with $\phi(m) = (p-1)(q-1)$
- encrpytion of cleartext t is $t^e \bmod m$
- decryption of ciphertext c is $c^A \bmod m$ where A, B such that $A \cdot e + B \cdot \phi(m) = 1$, compute A, B by extended Euclidean algorithm
- proof: $Ae \equiv 1 \bmod \phi(m)$, thus $(c^e)^A \equiv c^1$ using Fermat's "little" theorem $c^{\phi(m)} \equiv 1 \bmod m$
- Ex: $p = 3, q = 11,\ m = 33,\ e = 3, \phi(m) = 20,$ $A = 7, B = -1, 7 \overset{enc}{\to} 7^3 \equiv 13 \overset{dec}{\to} 13^7 \equiv 7.$

Experiment: break RSA encryption

- private key: (p, q) both prime
- public key: (e, m) where $m = pq$ and $\gcd(e, \phi(m)) = 1$ with $\phi(m) = (p-1)(q-1)$
- encrpytion of cleartext t is $t^e \bmod m$
- decryption of ciphertext c is $c^A \bmod m$ where A, B such that $A \cdot e + B \cdot \phi(m) = 1$, compute A, B by extended Euclidean algorithm
- proof: $Ae \equiv 1 \bmod \phi(m)$, thus $(c^e)^A \equiv c^1$ using Fermat's "little" theorem $c^{\phi(m)} \equiv 1 \bmod m$
- Ex: $p = 3, q = 11,\ m = 33,\ e = 3, \phi(m) = 20,$ $A = 7, B = -1, 7 \overset{enc}{\to} 7^3 \equiv 13 \overset{dec}{\to} 13^7 \equiv 7.$

Extended Euclidean Algorithm

- Theorem: for $a, b \in \mathbb{Z}$ there exist $c, d \in \mathbb{Z}$ such that $ac + bd = \gcd(a, b)$
- Proof: modify Euclid's algorithm (for computing $\gcd(a, b)$) in such a way that it also computes c, d.

Extended Euclidean Algorithm

- Theorem: for $a, b \in \mathbb{Z}$ there exist $c, d \in \mathbb{Z}$ such that $ac + bd = \gcd(a, b)$
- Proof: modify Euclid's algorithm (for computing $\gcd(a, b)$) in such a way that it also computes c, d.

Experiment: break Diffie-Hellman

- common, public: base g, prime modulus p
- A's secret is number a, send $g^a \bmod p$ to B
- B's secret is number b, send $g^b \bmod p$ to A
- shared secret then is $s = (g^a)^b = (g^b)^a \bmod p$
- use s for standard (symmetric) encryption
- Ex: $g = 2, p = 19$,
  $a = 11, g^a = 15$, $b = 12, g^b = 11$,
  $s = g^{11 \cdot 12} = 7 \bmod 19$.

Experiment: break Diffie-Hellman

- common, public: base g, prime modulus p
- A's secret is number a, send g^a mod p to B
- B's secret is number b, send g^b mod p to A
- shared secret then is $s = (g^a)^b = (g^b)^a \bmod p$
- use s for standard (symmetric) encryption
- Ex: $g = 2, p = 19$,
  $a = 11, g^a = 15$, $b = 12, g^b = 11$,
  $s = g^{11 \cdot 12} = 7 \bmod 19$.

Experiment: break Diffie-Hellman

- common, public: base g, prime modulus p
- A's secret is number a, send g^a mod p to B
- B's secret is number b, send g^b mod p to A
- shared secret then is $s = (g^a)^b = (g^b)^a \bmod p$
- use s for standard (symmetric) encryption
- Ex: $g = 2, p = 19$,
  $a = 11, g^a = 15$, $b = 12, g^b = 11$,
  $s = g^{11 \cdot 12} = 7 \bmod 19$.

Experiment: break Diffie-Hellman

- common, public: base g, prime modulus p
- A's secret is number a, send $g^a \bmod p$ to B
- B's secret is number b, send $g^b \bmod p$ to A
- shared secret then is $s = (g^a)^b = (g^b)^a \bmod p$
- use s for standard (symmetric) encryption
- Ex: $g = 2, p = 19$,
  $a = 11, g^a = 15$, $b = 12, g^b = 11$,
  $s = g^{11 \cdot 12} = 7 \bmod 19$.

Experiment: break Diffie-Hellman

- common, public: base g, prime modulus p
- A's secret is number a, send $g^a \bmod p$ to B
- B's secret is number b, send $g^b \bmod p$ to A
- shared secret then is $s = (g^a)^b = (g^b)^a \bmod p$
- use s for standard (symmetric) encryption
- Ex: $g = 2, p = 19$,
  $a = 11, g^a = 15$, $b = 12, g^b = 11$,
  $s = g^{11 \cdot 12} = 7 \bmod 19$.

Experiment: break Diffie-Hellman

- common, public: base g, prime modulus p
- A's secret is number a, send g^a mod p to B
- B's secret is number b, send g^b mod p to A
- shared secret then is $s = (g^a)^b = (g^b)^a$ mod p
- use s for standard (symmetric) encryption
- Ex: $g = 2, p = 19$,
  $a = 11, g^a = 15$, $b = 12, g^b = 11$,
  $s = g^{11 \cdot 12} = 7$ mod 19.