Countermeasures 8

# Personal information and the infringement of rights

The phrase “big data” came into use several years ago. Simply put, big data means that it has become possible to rapidly analyze large volumes of data, so we should gather various types of data, and effectively use it in business activities. For example, the history of user behavior at an online shop is analyzed to produce ad recommendations, social media information is analyzed to display possible acquaintances, regular location information is analyzed to provide weather and traffic information for a person's place of work or home, and your location information, history of searches/entries/language changes on a website, information when an error occurred, and various other forms of information can now be collected to improve services and applications.

Furthermore, it has become possible to easily search and access information, images, music, video, and other content. In addition, content can be easily posted and shared on blogs, social media, etc.

With big data gaining momentum and content becoming easy to post and share in recent years, how should we approach the internet? This section explains what you should pay attention to in order to avoid having your personal information misused or your privacy violated and to make sure that you do not infringe another person’s rights or commit an unlawful act.

## 4 key points regarding personal information and the infringement of rights

**8-1** Check the information that is gathered by PCs and smartphones

**8-2** Check the degree to which your website browsing history is shared

**8-3** Beware of making personal information public on social media

**8-4** Be conscious of the rights and laws concerning intellectual property and personal information, etc.

## 8-1 Check the information that is gathered by PCs and smartphones

The usage history and other information is actively gathered from Google accounts, Apple IDs, Microsoft accounts, and other accounts that are shared across PCs and smartphones, so there is a possibility that some information which the user may prefer not to provide is also being collected. In Android, iOS, Windows 10 and later versions, various types of information are gathered when the user selects the settings recommended by the provider as the default. Carefully check the privacy settings and restrict them to the information that you are comfortable providing.

### Privacy settings in each OS

■**Windows 10**

[Settings] > [Privacy]

■**macOS**

[System Preferences] > [Security & Privacy] > [Privacy]

■**iOS**

[Settings] > [Privacy]

■**Android**

[Settings] > [Google] > [Google Account]
[Settings] > [Apps] > (Open each app) > [PERMISSIONS]

## 8-2 Check the degree to which your website browsing history is shared

Using a web browser to search websites, browse, and use web services integrates a lot of information concerning the user's business and privacy such as money management information, business information, individual tastes and thoughts, etc.

A PC which is shared with another user retains not only the website browsing history and other information but also the authentication information (logged-in status). **This means that not only can your history information be viewed by another**

**person, but there is also a risk that the PC may log back into web services that you were using. To prevent such information from remaining on a shared PC, be sure to use the private browsing feature of the web browser when using web services.** (Each of the browsers use a different name. Internet Explorer 11 and Edge have InPrivate Browsing, Chrome has Incognito mode, Firefox has Private Browsing, and Safari has Private Browsing.) After you are finished using the web services, be sure to log out and exit the web browser.

Furthermore, web browsers that link accounts with cloud services such as Edge (Microsoft accounts), Chrome (Google accounts), and Safari (Apple IDs) upload (save) the website browsing history, bookmarks, IDs, passwords, etc. to the cloud. While this feature makes such information available from any device, the browsing history, etc. is also utilized for big data in some cases. Carefully check the web browser and cloud service privacy settings and turn off any items that you do not wish to upload from your PC, smartphone, tablet, etc.

## 8-3 Beware of making personal information public on social media

Regarding the ethics and use of social media, please read the “Five Key Points That You Should Know When Using Social Media” (Social Media Guidelines) for students, because it is an extremely useful reference.

Caution is required when using social media not only from the perspective that your personal information may be abused, but also because of the added possibility that the private information of your friends may also be abused (through information posted by you and your social media connections). In particular, there is a possibility that an individual may be identified by combining multiple types of information such as the background which appears in an uploaded photo, etc. **Please be aware that even if an individual cannot be identified from one post, there are cases where it is possible to identify an individual through a combination of posts.**

Furthermore, personal information is being unintentionally published (mainly due to a lack of understanding of social media/service rules or technology) on social media in an increasing number of cases.

### Examples of personal information being unintentionally published

- Using services without checking the scope of sharing
- Setting the scope of sharing incorrectly
- Not realizing that location information is included in photos and posts
- A friend who shared your post re-shared and published the content
- Not checking if the social media operator is collecting post content and other information and using it for unintended purposes or providing it to third parties

An increasing number of clever methods exploit such information to identify an individual and send targeted attack emails or commit fraud. **Because it is difficult to detect such elaborate methods, be sure to carefully check the social media features, scope of sharing, terms of service, and privacy policy (see Countermeasures 9-2. “Check how personal information is handled”) to avoid unintentionally publishing personal information.**

Ref: Ritsumeikan University, SNS利用にあたって知ってもらいたい5つのこと、SNSガイドライン(Five Key Points That You Should Know When Using Social Media, Social Media Guidelines)[19]
http://www.ritsumei.ac.jp/rs/sns/

Ref: Ministry of Internal Affairs and Communications, 国民のための情報セキュリティサイト「SNS利用上の注意点」(“Precautions When Using Social Media” information security site for citizens)[20]
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/05.html

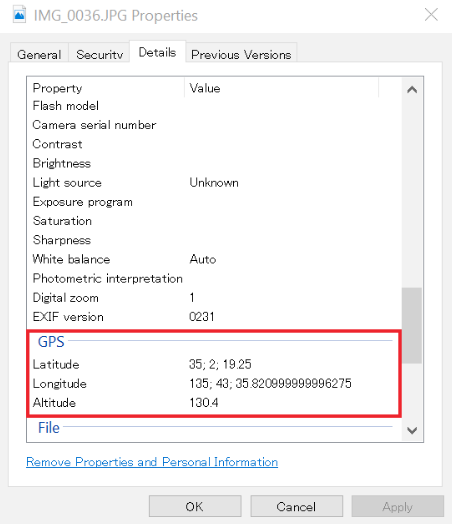
Ref: Nikkei BP, SNSの落とし穴：こんなはずじゃなかった！SNSで個人情報がダダ漏れ、取り返しのつかないことに (Social media pitfalls: This was not supposed to happen! Massive leaks of personal information on social media cannot be undone)[21]
http://www.nikkeibp.co.jp/article/matome/20131125/374827/

[19,20] This website is Japanese only.
[21] This website is currently unavailable.

Explanation ⑫

## Location acquisition features and location information embedded in images

When a photo is taken on a device that can acquire the location information (mobilephones, smartphones, and some digital cameras), the information about where that photo was taken is embedded in the image (This feature is called “geotagging.” The figure below shows the information embedded by the iPhone camera when the image properties are checked on a Windows computer. The latitude and longitude information is displayed.). With the latitude and longitude information, the location can be easily determined with a map app.



IMG_0036.JPG Properties

| Property | Value |
|---|---|
| Flash model | |
| Camera serial number | |
| Contrast | |
| Brightness | |
| Light source | Unknown |
| Exposure program | |
| Saturation | |
| Sharpness | |
| White balance | Auto |
| Photometric interpretation | |
| Digital zoom | 1 |
| EXIF version | 0231 |
| GPS | |
| Latitude | 35; 2; 19.25 |
| Longitude | 135; 43; 35.820999999996275 |
| Altitude | 130.4 |
| File | |

Remove Properties and Personal Information

Figure 23 Properties of a photo taken with an iPhone

There are also cases where the Twitter social media app published location information in tweets, etc. By comparing the location where a photo was taken, the location where it was posted, and the post content, it is possible to determine the type of location (home, etc.).

**<Example: “Taking a photo of a cat at home and posting it”>**

User A uses her real name on social media. One day, User A took a photo of her cat at home with a smartphone and published it on social media. Several days later, fake invoices, etc. started arriving at User A's home.

In addition, a person's home and place of work can be inferred through behavioral analysis. Be especially careful about location information when using social media.

Tips⑩

## Secret questions and social media

In Countermeasures 4 “Email,” we introduced cases where social media containing various information about a particular individual is used as preparation for targeted attack emails and fraud. Using a similar line of thinking, you should also be careful about “secret questions” and social media.

“Secret questions” are a feature for verifying the identity of a user by entering questions determined in advance during user registration, etc. that only the actual person would know, and this feature is used during procedures to reissue a password or send notifications to a user who has forgotten their password. These questions might include, “What is your mother’s maiden name?”, “What is your favorite food?”, and “What is your pet’s name?” These secret questions appear to be an effective way to confirm a person's identity, but to be honest this method is extremely dangerous. It is dangerous, because this information is known by people who are familiar to you, **it becomes easier to guess when you are making various posts on social media, and you may be unintentionally publishing the answers to the secret questions.** Due to the risk that IDs and passwords may be easily stolen in this way, there are increasing calls to discontinue the use of “secret questions” as a system of authentication.

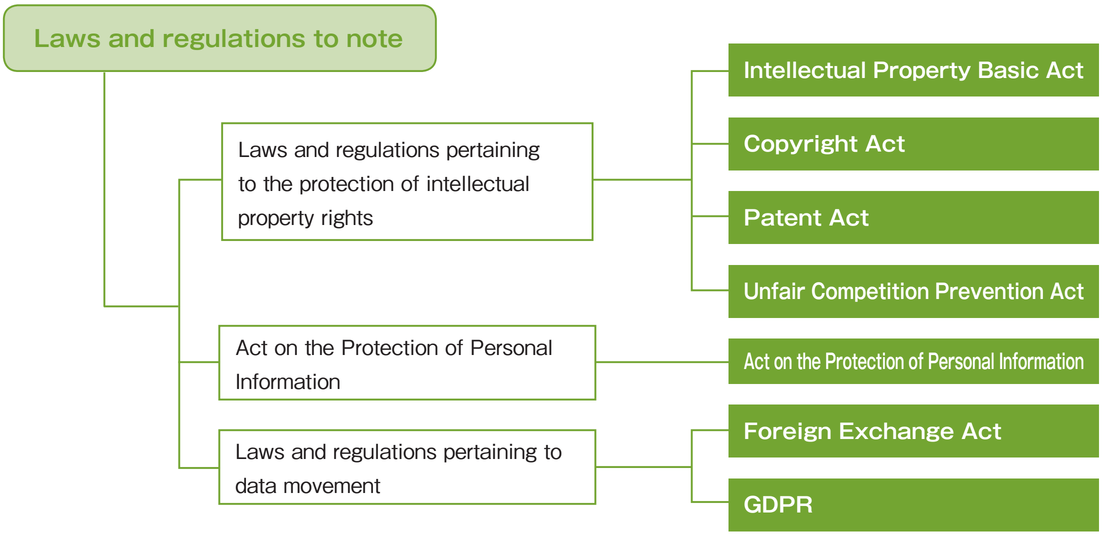
**When registering the answers to “secret questions,” do not use correct answers which may be guessed.**

Ref: IPA, “その秘密の質問の答えは第三者に推測されてしまうかもしれません (The Answer to That Secret Question May Be Guessed by a Third Party)”[22]
https://www.ipa.go.jp/security/txt/2015/07outline.html

[22] This website is Japanese only.

## 8-4 Be conscious of the rights and laws concerning intellectual property and personal information, etc.

The “Laws and regulations pertaining to the protection of intellectual property rights,” “Act on the Protection of Personal Information,” and the “Laws and regulations pertaining to data movement” are the three laws and regulations which you should be pay attention to when using the internet as shown in the figure below.


Laws and regulations to note
Laws and regulations pertaining to the protection of intellectual property rights
Act on the Protection of Personal Information
Laws and regulations pertaining to data movement
Intellectual Property Basic Act
Copyright Act
Patent Act
Unfair Competition Prevention Act
Act on the Protection of Personal Information
Foreign Exchange Act
GDPR

Citation source: 図解入門ビジネス最新ISO27001 2013の仕組みがよ～くわかる本
How - nual Business Guide Book on Understanding the Latest ISO27001 2013 System[23]

Figure 24 Laws and regulations to note

[23] This book is Japanese only.

First, we will take a look at the “Laws and regulations pertaining to the protection of intellectual property rights.” Due to the familiarity of the Internet, it has become extremely easy to obtain, duplicate, publish, and share images, music, movies, documents, and other typical content. These types of content have intellectual property rights as typified by copyright, and they are protected by laws and regulations. Under the Copyright Act, there is some tolerance regarding the use of works in classes and teaching materials “to the extent that this is found to be necessary for the purpose of school education” and “it is not-for-profit.” However, there are also cases where this is interpreted incorrectly, and the scope of usage is restricted by the usage license agreement. Consideration is needed not only for copyrights but also industrial property rights (trademark rights, patent rights, utility model rights, and design rights), trade secrets, and other general intellectual property rights. For example, if you publish a photo or video on the internet that shows the face of someone who has not provided consent, that would be an infringement of rights.

Secondly, the “Act on the Protection of Personal Information” is important to this university as an institution which handles a large amount of personal information. Under “The Ritsumeikan Trust Personal Information Protection Regulations[24]” (hereinafter, “Personal Information Protection Regulations”), faculty members are responsible for the appropriate management of personal information and shall comply with the regulations in educational research activities, operation management, and other duties based on a clear understanding of the Personal Information Protection Regulations, the Act on the Protection of Personal Information (hereinafter, “Personal Information Protection Act”), and the guidelines.

Thirdly, there is a tendency to overlook the “Laws and regulations pertaining to data movement,” so please be careful. The two important laws are the “Foreign Exchange and Foreign Trade Act” (hereinafter, “Foreign Exchange Act”) and the “General Data Protection Regulation” (EU General Data Protection Regulation, hereinafter, “GDPR”). The Foreign Exchange Act is designed from a national security export control perspective to prevent weapons and dual-use technologies from being delivered to specific regions. Information can easily cross national borders through the internet, so caution is required. The GDPR is a law for protecting personal information in the European Economic Area which is similar to the Japanese Personal Information Protection Act, but the rules are far more stringent than in Japan. In cases where personal information is acquired across borders from an individual located within the EEA area and in cases where personal information is transferred across borders from an area inside the EEA to an area outside the EEA, the GDPR standards must be satisfied, so caution is required.

[24] This English document is a translation of the original Japanese document and is for reference only.

In addition, although it is not clearly stated in the laws and regulations, the right of privacy and the right of likeness have been recognized as part of the right to the pursuit of happiness and personal rights under the concept of respect as individuals in Article 13 of the Japanese Constitution based on previous court precedents, and infringing on those rights is an unlawful act. Depending on the type of information (here we are referring to data and content), the usage may be legally regulated by a non-disclosure agreement (NDA) or product license agreement, etc.

To avoid infringing rights or committing an unlawful act, you should first **be aware that you are bound by various limits and restrictions when using data and content on the internet, so be sure to understand the restrictions regarding the extent to which you can use it, who you can show it to, etc.**

Next, **configure the appropriate access rights (see Countermeasures 6 “Access rights management”) according to the restrictions imposed on the information described above to** avoid information leaks caused by accidentally publishing or sharing **to the world of the internet where information is easily duplicated, published, and shared.**

Ref: General Incorporated Association Japan Copyright Educational Association, 著作権Q＆A (Copyright Q&A)[25]
http://jcea.info/Q&A.html

Ref: The Japan Universities Association for Computer Education, “教員のための個人情報活用ガイドライン(Guidelines for Faculty Use of Personal Information)”[26]
http://www.juce.jp/kojin_joho/
*Guidelines prior to the FY2017 amendments

Ref: Personal Information Protection Commission JAPAN
https://www.ppc.go.jp/en/index.html

[25,26] This website is Japanese only.

Explanation ⑬

## Information that must not cross national borders

As mentioned in the previous section, the "Foreign Exchange Act" and the "GDPR" are representative laws which regulate the transfer of information across national borders. While it is easy to picture physical goods crossing national borders, it might be a little difficult to imagine a situation in which information "must not be removed" or "must not be transferred across national borders" in the world of the Internet.

For example, if you were to take information regulated under the "Foreign Exchange Act" and accidentally publish it on the Internet, permit someone from a specific region to access it, or share it with someone who has citizenship from a specific region, **that information would still be subject to the same regulations even if it came from a server installed on campus.** Conversely, even if a cloud service or other data storage location (data center or other location where the cloud service data is actually located) is situated in a specific region, there is no problem if access from the specific region is regulated.

Meanwhile, under the "GDPR," the transfer of any and all information about an individual located within the EEA area to a third country outside of the EEA which does not have an "adequate level of protection (recognized by the EU as ensuring a sufficient level of data protection)" is restricted. As of 2018, Japan has not received this "adequacy decision," which means that you must check and comply with the GDPR standards when bringing information about individuals located in the EEA area that was collected in that area to Japan (to the university or cloud services that use a Japanese data center) or when collecting information from individuals including those within the EEA area. However, it is possible to manage the information using services provided under the contractual terms from Google, Amazon, Microsoft, etc. For more details, please carefully read the FAQ for each service.

Ref: 立命館大学の安全保障輸出管理関連の資料・様式等 (Ritsumeikan University Documents and Forms Pertaining to National Security Export Controls)[27]
http://www.ritsumei.ac.jp/research/member/study_ethic/se15.html/

[27] This website is Japanese only.