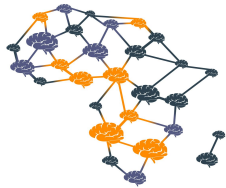


Neuroimaging Data Collection and Sharing: Ethical and Legal Considerations

EEG Workshop 2025

Damian Eke



African
Brain
Data
Network



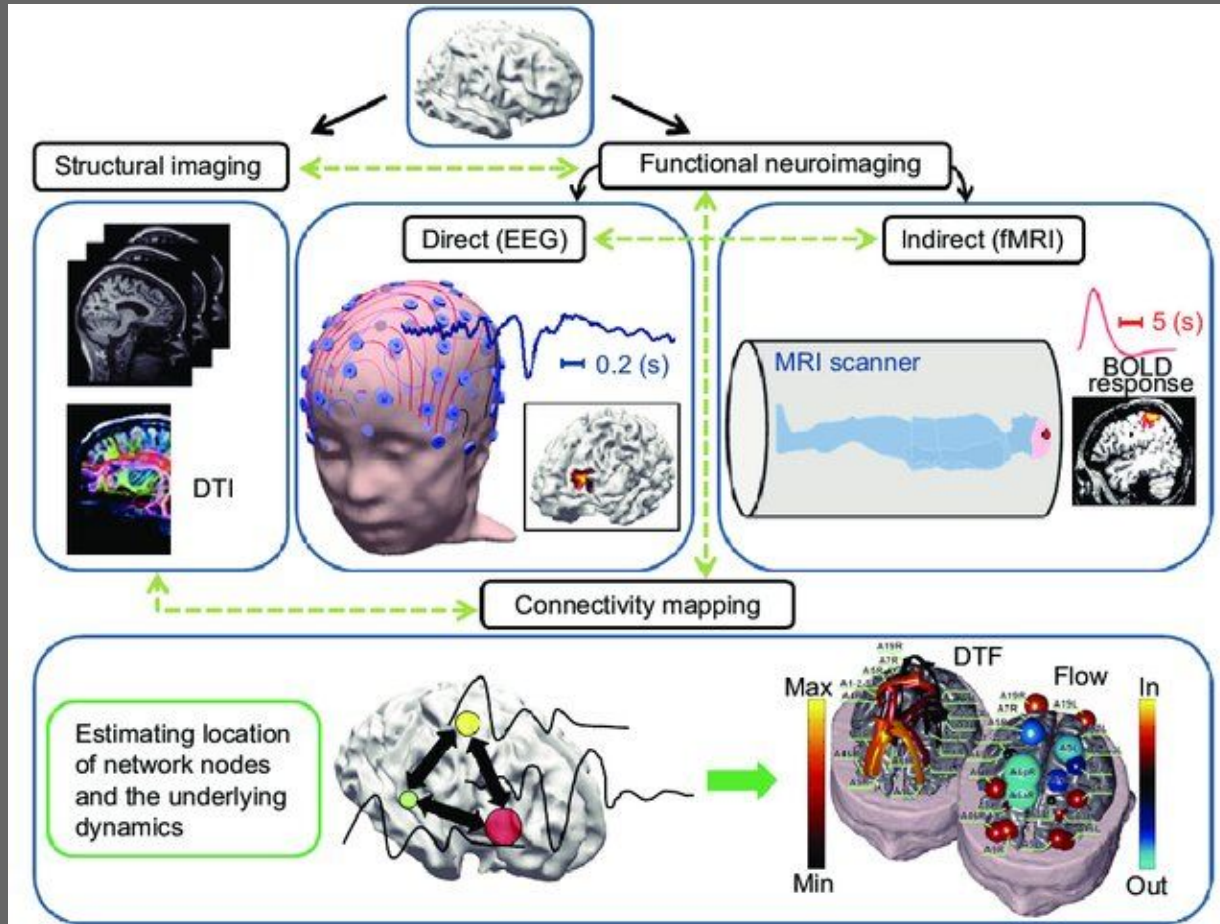
THE
KAVLI
FOUNDATION



University of
Nottingham

UK | CHINA | MALAYSIA

Neuroimaging modalities



Ethical issues to consider in Neuroimaging data Collection and Sharing

Informed Consent

- Sufficient Information
- Comprehension
- Voluntariness

Respect for autonomy

Participants have the right to make informed decisions about their involvement



Process of Informed Consent

Ethics review process

- Prepare your information Sheet and the consent form
 - Aims and objectives
 - Entire research process in a language accessible to non experts
 - Participants' involvement (including their right to withdraw at any time)
 - Risks and Benefits
 - Data management processes
- Application for ethics approval from ERB
- Get signatures
 - From patients
 - Guardians
 - Carers
 - Next of kin

Privacy and Confidentiality

- Neuroimaging data often reveal detailed personal information about an individual's
 - Names
 - Age
 - Occupation
 - Address
 - Brain structure and function (Brain prints)

Respect for privacy

Researchers must take measures to safeguard participants' identity and sensitive information

Protection of privacy

Irreversible removal of personally identifiable information (PII) from datasets (both direct and indirect identifiers)



Removal of direct identifiers from the datasets to protect the confidentiality of the data subjects



BrainPrint: EEG biometric identification based on analyzing brain connectivity graphs

Min Wang  , Jiankun Hu , Hussein A. Abbass 

Show more 

 Add to Mendeley  Share  Cite

<https://doi.org/10.1016/j.patcog.2020.107381> 

[Get rights and content](#) 

Highlights

- The topological features of brain connectivity graphs can be effectively used for EEG biometric identification.
- Seven connectivity metrics including a new one defined on the algorithmic complexity of signals, and twelve graph features are

Article | [Open access](#) | Published: 11 October 2022

Person-identifying brainprints are stably embedded in EEG mindprints

[Yao-Yuan Yang](#), [Angel Hsing-Chi Hwang](#), [Chien-Te Wu](#)  & [Tsung-Ren Huang](#) 

[Scientific Reports](#) **12**, Article number: 17031 (2022) | [Cite this article](#)

2976 Accesses | **5** Citations | **4** Altmetric | [Metrics](#)

Abstract

Electroencephalography (EEG) signals measured under fixed conditions have been exploited as biometric identifiers. However, what contributes to the uniqueness of one's brain signals remains unclear. In the present research, we conducted a multi-task and multi-week EEG study with ten pairs of monozygotic (MZ) twins to examine the nature and components of person-identifiable brain signals. Through machine-learning analyses, we uncovered a person-identifying EEG component that served as "base signals" shared across tasks and weeks. Such task invariance and temporal stability suggest that these person-identifying EEG characteristics are more of structural brainprints than functional mindprints. Moreover, while

Article | [Open access](#) | Published: 22 August 2022

Brainprints: identifying individuals from magnetoencephalograms

[Shenghao Wu](#), [Aaditya Ramdas](#) & [Leila Wehbe](#) 

[Communications Biology](#) **5**, Article number: 852 (2022) | [Cite this article](#)

3187 Accesses | **5** Citations | **2** Altmetric | [Metrics](#)

Abstract

Magnetoencephalography (MEG) is used to study a wide variety of cognitive processes. Increasingly, researchers are adopting principles of open science and releasing their MEG data. While essential for reproducibility, sharing MEG data has unforeseen privacy risks. Individual differences may make a participant identifiable from their anonymized recordings. However, our ability to identify individuals based on these individual differences has not yet been assessed. Here, we propose interpretable MEG features to characterize individual difference. We term these features brainprints (brain fingerprints). We show through several datasets that brainprints accurately identify individuals across days, tasks, and even between MEG and Electroencephalography (EEG). Furthermore, we identify consistent brainprint components that are important for identification. We study the dependence of identifiability on the amount of data available. We also relate identifiability to the level of

Estimating the success of re-identifications in incomplete datasets using generative models

[Luc Rocher](#), [Julien M. Hendrickx](#) & [Yves-Alexandre de Montjoye](#) 

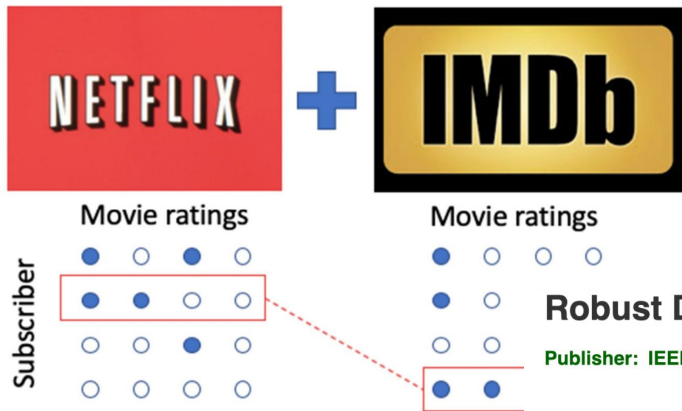
[Nature Communications](#) **10**, Article number: 3069 (2019) | [Cite this article](#)

182k Accesses | **432** Citations | **2675** Altmetric | [Metrics](#)

Abstract

While rich medical, behavioral, and socio-demographic data are key to modern data-driven research, their collection and use raise legitimate privacy concerns. Anonymizing datasets through de-identification and sampling before sharing them has been the main tool used to address those concerns. We here propose a generative copula-based method that can accurately estimate the likelihood of a specific person to be correctly re-identified, even in a heavily incomplete dataset. On 210 populations, our method obtains AUC scores for predicting individual uniqueness ranging from 0.84 to 0.97, with low false-discovery rate.

Using our model, we find that 99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes. Our results suggest that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by GDPR and seriously challenge the technical and legal adequacy of the de-identification release-and-forget model.



<https://ieeexplore.ieee.org/document/4531148>

Robust De-anonymization of Large Sparse Datasets

Publisher: IEEE Cite This PDF

Arvind Narayanan ; Vitaly Shmatikov All Authors

1311

Cites in
Papers

25

Cites in
Patents

12463

Full
Text Views



Abstract

Document Sections

- 1 Introduction
- 2 Related work
- 3 Model
- 4 De-anonymization algorithm
- 5 Case study: Netflix Prize dataset

Abstract:

We present a new class of statistical de- anonymization attacks against high-dimensional micro-data, such as individual preferences, recommendations, transaction records and so on. Our techniques are robust to perturbation in the data and tolerate some mistakes in the adversary's background knowledge. We apply our de-anonymization methodology to the Netflix Prize dataset, which contains anonymous movie ratings of 500,000 subscribers of Netflix, the world's largest online movie rental service. We demonstrate that an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber's record in the dataset. Using the Internet Movie Database as the source of background knowledge, we successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information.

Published in: 2008 IEEE Symposium on Security and Privacy (sp 2008)

Opinion

Sport

Culture

Lifestyle



politics UK Climate crisis Middle East Ukraine Environment Science Global development Football **Tech** Business Obituaries

d computer
y

🕒 This article is more than **7 years old**

'Anonymous' browsing data can be easily exposed, researchers reveal

A journalist and a data scientist secured data from three million users easily by creating a fake marketing company, and were able to de-anonymise many users



n in Las Vegas

17 07.00 BST

Advertisement

For page turners
This Christmas,
give someone 64 pages
of award-winning
journalism

EU General Data Protection Regulation (GDPR)

GDPR applies to the processing of personal data

Data processing - "any operation or set of operations which are performed on personal data"

Personal Data is any information relating to an identified or identifiable person

Recital 26 – Identifiable – If anyone can identify a natural person using all means reasonably likely to be used, then the information is personal data.

GDPR

‘General Personal Data’: Names, telephone numbers, email addresses, identification numbers, account related data such as Human Resources data, location data, IP addresses.

‘Special category Personal Data’:

- A. personal data revealing racial or ethnic origin,
- B. political opinions,
- C. religious or philosophical beliefs,
- D. trade union membership,
- E. genetic data,
- F. biometric data for the purpose of uniquely identifying a natural person,
- G. data concerning health**
- H. data concerning a natural person's sex life or sexual orientation.

Includes:

- Pseudonymised/De-identified Data

Excludes:

- Anonymised Data
- Post-mortem data
- Animal data

What do you do?

- Legal basis for processing
- Technical and Organisational Measures
 - Data Protection Impact Assessment (DPIA)
 - Anonymisation/Pseudonymisation
 - Encryption
- Relevant Agreements
 - Data use agreements
 - Data Transfer Agreements
 - Data processing agreement
 - Joint Data controllership agreement



Identify Lawful Basis art. 6

Consent- Clear Consent
for a clear purpose

Contract – necessary for a
contract with the
individual

Legal Obligation –
Necessary to comply
with the law

Vital Interests –
Necessary to protect
someone's life

Public Task – necessary to
perform a task in the public
interest, or an official
function, and is necessary in
law

Legitimate interest –
necessary for our legitimate
interest, unless there's a
good reason to protect
someone's personal data

Lawful Basis (art. 9)

Explicit Consent

Made public by the data subject

Public interest in the area of public health

Substantial public interest on the basis of union or state law

Employment

Carried out by a not for profit organisation (e.g religious organisation or trade union)

Preventive or occupational medicine, inc. to assess the working capacity of the employee

Vital Interests

Legal Claims

Archiving purposes in public interest, scientific or historical research purposes or statistical purposes

One lawful basis is always required under Article 6 (General processing)

For special category data, in addition to a lawful basis under Article 6, a lawful basis is required under Article 9

Criminal offence data requires a lawful basis under Article 6 AND the processor must have an official authority to process the data (GDPR Article 10 and the DPA 2018) and have a policy

Also consider GDPR principles (including information security)

Need to comply with Privacy & Electronic Communications Regulations (PECR)

Need to consider
Common law duty of confidence
Human Rights Act (Article 8)

Data Subject Rights

The right to be informed – always applies

The right of access – always applies

The right to rectification – always applies

The right to erasure

The right to restrict processing

The right to data portability

The right to object

Rights in relation to automated decision making and profiling.

Lawful Basis and data subject rights

Think about whether you can comply with these rights when determining the legal basis.
Consider resource implications.

Select only one lawful basis under Article 6. Think about whether you can comply with these rights when determining the legal basis. You must consider the resource implications.	RIGHT TO ERASURE	RIGHT TO PORTABILITY	RIGHT TO OBJECT
CONSENT	☒	☒	Right to withdraw consent
CONTRACT	☒	☒	☒
LEGAL OBLIGATION	☒	☒	☒
VITAL INTERESTS	☒	☒	☒
PUBLIC TASK	☒	☒	☒
LEGITIMATE INTERESTS	☒	☒	☒

Create Organisational Safeguards

Relevant Agreements

- Data use agreements
- Data Transfer Agreements
- Data processing agreement
- Joint Data controllership agreement

Chapter 5

Transfers of personal data to third countries or international organisations

Article 44 – General principle for transfers

Article 45 – Transfers on the basis of an adequacy decision

Article 46 – Transfers subject to appropriate safeguards

Article 47 – Binding corporate rules

Article 48 – Transfers or disclosures not authorised by Union law

Article 49 – Derogations for specific situations

Article 50 – International cooperation for the protection of personal data

Establish Technical Measures

- Anonymisation/Pseudonymisation
- Encryption



International Transfers

- Data sovereignty is prioritised.
- International Transfers can occur only when the when the recipient of the personal data is subject either to
 - (1) a law
 - (2) Binding Corporate Rules ('BCRs'),
 - (3) contractual clauses,
 - (4) a Code of Conduct, or
 - (5) a certification mechanism that "affords an adequate level of protection" to that provided by the Act.

Key Points to Note...

- Regulations are not an excuse for not sharing your data
- Consent for the research protocol is different from consent as a lawful basis
- Consent is not the only lawful basis and is not usually the only lawful basis
- Always remember your duties to the data subjects

	Raw	Pseudonymous			Anonymous	
	Personal	Key coded	Pseudonymous	De-identified	Anonymous	Aggregated anonymous
Direct identifiers 	Intact	Eliminated or transformed	Eliminated or transformed	Eliminated or transformed	Eliminated or transformed	Eliminated or transformed
Indirect identifiers 	Intact	Intact or partially intact	Intact or partially intact	Partially intact	Eliminated or transformed	Eliminated or transformed
Re-identification 	High probability	Medium probability	Medium probability	Low probability	Not Possible	Not Possible
						

Who owns the neuroimages you collect?

Data controllers and processors

Data controller: an individual, private entity, public Commission or agency, or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor: an individual, private entity, public authority, or any other body who or which processes personal data on behalf of or at the direction of a data controller or another data processor.

When the controller collects personal data directly or indirectly from a data subject, they must supply the data subject with the following information prior to collection:

- The identity, residence or place of business of, and means of communication with the controller;
- The specific lawful basis of processing under either Section 25(1) or 30(1) of the Act, and the specific purposes of processing;
- The categories of recipients of the personal data;
- The existence of the data subject rights;
- The retention period of the data;
- The right to lodge a complaint with the Commission; and
- The existence of any automated decision-making, including profiling, its significance, the envisaged consequence of such processing for the data subject, and the right to object to/challenge such processing.

Non-representative subject selection - Selection Bias

- You should avoid selection bias as well as exploiting vulnerable populations and ensure that the selection of subjects is fair and equitable
- Neuroimaging studies should be conducted with scientific rigor to ensure the validity and reliability of the results

Ethical Principle: Justice. Ensure fair distribution of the benefits and burdens of research and avoid exploitation

Dual-Use of Concern

Neuroimaging technologies could potentially be misused for purposes such as

- Mind-Reading and Privacy Invasion
- Manipulation of Brain Activity
- Military and Intelligence Applications

Ethical Principle: Responsible conduct/Beneficence/Non-Maleficence. Researchers should consider the potential dual-use implications of their work and take steps to mitigate risks

*Thank
you!*

Questions?