APPENDIX A

GDPR CONTENT ANALYSIS

TABLE VI
TABLE OF COHEN'S KAPPA BETWEEN RATERS FOR GDPR SQC ANALYSIS FOR EACH MAIN CATEGORY

Category\ Rater	Rater 1 & 2	Rater 1 & 3	Rater 2 & 3
1. Data Subjects	1	1	1
2. Data Type	0.72	0.69	0.68
3. Data Processing	0.66	0.67	0.69
4. Purpose	0.78	0.76	0.73
5. Security	0.59	0.37	0.46

TABLE VII
TABLE OF COHEN'S KAPPA BETWEEN RATERS FOR THE GDPR SQC ANALYSIS WITH AND WITHOUT THE SECURITY CATEGORY

	Rater 1	**Rater 2**	**Rater 3**
Rater 1		0.72/0.72	0.69/0.72
Rater 2	0.72/0.72		0.70/0.72
Rater 3	0.69/0.72	0.70/0.72	

TABLE VIII
OVERVIEW OF THE TAXONOMY RESULTING FROM THE SQC

1. Data Subject	2. Data Type	3. Data Processing	4. Processing Purpose	5. Security
1.1 Vulnerable Data Subject	2.1 Personal Data	3.1 Data Processing on a Large Scale	*4.1 Commercial or Business Purposes*	5.1 Technical Measures
1.1.1 Children	2.1.1 Sensitive Data	3.2 Data Collection	4.1.1 Marketing	*5.1.1 Access Control*
1.1.2. Impaired Data Subjects	2.1.1.1 Racial or Ethnic Origin Data	3.3 Data Recording	*4.1.2 Sale of Data*	*5.1.2. Hardware*
1.2. Other Data Subjects	2.1.1.2 Political Opinion Data	3.4 Monitoring	4.2 Research	*5.1.2.1 Data Location*
	2.1.1.3 Religious Beliefs Data	3.4.1 Systematic Monitoring on a Large Scale	4.2.1 Scientific Research	*5.1.2.2 Location of Processing*
	2.1.1.4 Philosophical Beliefs Data	3.4.2 Systematic Monitoring of a Publicly Accessible Area	4.2.2 Historical Research	*5.1.2.2.1 Centralized Processing*
	2.1.1.5 Trade Union Membership Data	3.4.3 Monitoring of the behavior of the data subjects	4.3 Statistical Purposes	*5.1.2.2.2 Distributed Processing*
	2.1.1.6 Genetic Data	3.5 Data Storage	*4.4. Service Provision*	*5.1.3 Software*
	2.1.1.7 Biometric Data	3.5.1 Storage Period	*4.5. Service Optimization*	*5.1.3.1 Encryption*
	2.1.1.8 Health Data	3.6 Data Combination		5.2 Organizational Measures
	2.1.1.9 Sex Life/Sexual Orientation Data	3.7 Profiling		*5.2.1 Certification*
	2.1.2 Criminal Conviction/Offenses Data	3.8 Automated Decision Making		*5.2.2 Education and Training*
	2.1.3 Employment Data	3.9 Data Alteration		
	2.1.4 Unique Identifiers	3.9.1 Data Adaptation		
	2.1.5 Financial Information	3.9.2 Data Rectification		
	2.1.6 Location Data	3.10 Data Alignment		
	2.2 Non-Personal Data	*3.11. Data De-Identification*		
		3.11.1 Pseudonymization		
		3.11.2 Anonymization		
		3.12 Data Disclosure		
		3.12.1 Data Transmission		
		3.12.2 Data Dissemination		
		3.12.3 Made Available Otherwise		
		3.12.4 Data Transfer to a Third Country		
		3.13 Restriction of Data Processing		
		3.14 Data Erasure		
		3.14.1 Data Destruction		

APPENDIX B

EXPERT INTERVIEW QUESTIONS

Demographic Questions:

1. Which disciplines did you study during your academic career?

2. What do you do professionally?

    a. How long have you been doing this?

    b. In what context do you come into contact with data protection issues?

Subject-specific Questions (What are potential sources of data protection risk?):

3. What information would be relevant for the user to learn?

4. Imagine now that you would have to summarize the information you just listed into super-categories. Into which categories would you divide this information?

5. We will now list you the main categories we have developed and would like to ask you to consider what possible subcategories/information you could think of and consider particularly relevant.

    a. Data subjects,

    b. Types of Data,

    c. Data Processing,

    d. Purposes of der Data Processing

    e. Security

6. Imagine that you could communicate only a fraction of the information you have just gathered to users. What information would you prioritize?

    a. Why do you think this information is especially relevant?

Subject-specific Questions (What are potential adverse consequences?):

7. When it comes to possible consequences for users with regard to their privacy, what global super-categories would you choose?

8. What could be specific adverse consequences that would be part of the super-categories you mentioned?

Subject-specific Questions (How can it happen?):

9. What causes can you think of that could lead to adverse consequences for users?

10. Would you consider possible negative consequences with respect to specific scenarios or across different contexts?

11. Which scenarios or context would you consider?

Subject-specific Questions (How likely is it to happen?):

12. In your opinion, what increases the likelihood of negative consequences occurring?

Specific questions for IT experts and lawyers (cluster analyses):

13. The topic “security” plays an important role in the handling of data. Which aspects would you include in the super-category “security”?

a. Which are especially relevant in the context of data protection?

b. How do you assess the relationship between software, hardware and organizational measures with regard to security?

APPENDIX C

RESULTS OF THE SYSTEMATIC QUALITATIVE CONTENT ANALYSIS OF EXPERT INTERVIEWS

TABLE IX
LATENT CONSEQUENCES

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
Informational Power	concentration of power as a result of information imbalances that can be used as an instrument for state and private power adapted from [1, p. 254]	17	17	general	Data Collection & Data Storage, Emergence of Information	Large Scale Processing	With data controllers collecting and gathering more data about data subjects and using this data to draw inferences about data subjects with or without their knowledge, the information asymmetry changes between controllers and data subjects at the expense of the data subjects. As access to more information also results in more possibilities regarding information generation, the result is a self-reinforcing process of information power.	Calo and Rosenblatt [2] argue that platforms like Airbnb, Lyft, and Uber possess deeply asymmetric information about and power over consumers and other participants in the sharing economy and use this power to leverage their access to information about users and their control over the user experience to mislead, coerce, or otherwise disadvantage sharing economy participants. As these companies can design their own information environment, track consumer behaviour within it, and change the conditions throughout that environment based on their observations, they have multiple possibilities to reach consumers at their most vulnerable, nudge them into overconsumption, and charge each consumer the most she may be willing to pay.	I see the causes first and foremost in the existing social structures of domination. That's where they are created, and then they reproduce themselves in the digital space, too. That's why they have their origin in the processing, that is, the collection and processing of data. So that's where the real origin is. Yes, it is not the stupidity of users. That's not what you just said either. Yes, I'm just saying it because that's how it's often communicated. So, first and foremost, I see the cause in the data-processing organizations, whether they are state authorities and agencies or companies. And also in the way digital markets are structured and regulated or deregulated. (15T)
Decontextualization	cross-sectoral usage of personal information characterized by surprising effects and lack of controllability [1, p. 301]	14	11	general	Emergence of Information		If new data is created from existing data (e.g., through prediction and classification) this changes the context according to contextual model of perceived risk, as the set of contextually agreed upon types of data is expanded. An example would be if non-medical data is used to predict medical data (see corresponding quote).	Facebook claimed to be able do deduce the emotional state of young people based on their posts, pictures, interactions and internet activity in real-time [3].	Any medical diagnosis of mine is, of course, health data. My typing speed on my mobile phone is just common data. But if the probability that I will suffer depression based on my typing speed is calculated, then of course this data processing also makes my typing speed health data. Or rather: this prognosis about my probability of depression is of course then a health date. Here again we have this phenomenon that we cannot differentiate only according to the types of data, but must also think about the algorithm perspective, because only through the associated algorithm, which makes a depression probability out of my typing speed, does this seemingly harmless data become health data. (91T)

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
			4		Data Disclosure		When a change in sender and receiver occurs, this marks a change of context according to the contextual model for perceived risk.	Facebook allowed Netflix and Spotify to access the app users' private messages who could use this data for their own purposes [4].	Once you have information in another context, it's very hard to control that information, and so I always focus on the primary purpose of the data collection versus other secondary purposes, secondary uses of the data over which far less control can be exerted. (42)
			4		Processing for other Purposes		When information is used for a purpose different to those originally agreed upon, this marks a change of context according to the contextual model for perceived risk.	Uber used a tool called "God View" that displayed all waiting users and active drivers in a given area. The original purpose of this tool originally was to assist management tasks in real time, employees also used it to spy on politicians, celebrities and ex-girlfriends [5].	There was this scandal here with the Berlin police, where the police accessed data records of an ex-partner or something. That means that there are no security gaps, there is simply misuse of data and so on. (05T)
Emergence of Information	possibility of automatically drawing new, previously unavailable conclusions from various pieces of information [1, p. 304]	12	7	general	Data Combination, Re-Identification		New information about a data subject can emerge by combining previously unknown data with the existing data relating to a data subject. This can be done probabilistically by calculating which data subject is most likely to have created the data in question (based on data occurring in both data sets), which might result in inaccurate data combination. Accurate data combination can be achieved through deterministic matching using a unique identifier, such as a cookie id, an IP address, a browser fingerprint, a device id, a user account id (like the “advertising IDs" used by Google, Apple, Microsoft, and Roku) or proprietary IDs (used by data companies like Acxiom, Experian, and Oracle).	In 2022 it was published that the queer dating platform grindr had sold the location information of its users since at least 2017. While the data did not contain personal information such as names or phone numbers, the data could still be matched by buyers of this data, who had access to the location information of their users by checking for communalities in the location data. Thus, on an individual level, being able to match a grindr user to an existing user from another service allows inference about their sexual preference without having to apply actual inference techniques [6]. On a collective level, matching common device locations from users allowed for the emergence of information about romantic encounters between specific users [7].	It is problematic when it comes to [...] data aggregation, of course, when data sets are combined and then used either for predictive or for classificatory purposes, i.e. the two most important applications, especially of econometric analysis or machine learning. That's where these particular risks arise, because at the time of data collection, it's not at all clear what information is going to be generated in the end. (03T) And also the re-identification, so for example if you are on a network, for example on Twitter, and you are anonymous there or use a largely anonymous fake name, you can still be identified in other networks because of the data you leave there. I think it was already shown in a study from 2009, in which anonymous Twitter networks could be reassembled on another network, I think Flickr, simply by comparing the networks with each other and then taking information from the other network, depending on which data point was missing. (98T)
			3		Inference	Informational Power	Inference techniques can be used to derive or infer new data about the data subject through classification or prediction. As most predictive models first have to be fitted using existing	Studies show that gender, age, ethnicity, body weight, drug consumption habits, or emotional state can be inferred from eye tracking data [8]; personality, physical traits, geographical origin,	Then I have also noted the problem of information asymmetries. A problem with the massive processing of information or data by large companies is that the companies can then generate more

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
							data from other data subjects, the more (varied) data controllers applying inference techniques have access to, the more precise (and varied) their inferences can be, which is why inference profits from greater information asymmetry. Emergence of data through statistical inference is therefore additionally dependent on context-spanning data from other data subjects.	emotions, level of intoxication and sleepiness, or health condition can be inferred from voice data [9]; and activities, health condition, body features, or individual gait can be inferred from accelerometer data [10] if the entities processing the information have enough data to build sufficiently precise models.	information about a person than the person knows about themselves. And, so to speak, modern data processing reverses the information asymmetry that classically existed to a certain extent. (03T)
			6	health	Inference		see explanation above	The location data of a woman visiting an abortion clinic can be used to infer her likeliness to have gotten an abortion, which is why Google vowed to delete such location data from the users' location history in July 2022 [11].	So let me give you an example: Any medical finding of mine is, of course, a health datum per se. My typing speed on my cell phone is actually a common date. But if it calculates the probability that I will suffer from depression based on my typing speed, then of course this data processing also turns my typing speed into a health datum. Or rather, this prediction about my probability of depression is of course then a health date. That is, here again we have this phenomenon that we cannot differentiate at all only according to the type of datum, but have to think along this algorithm perspective, because only through the associated algorithm, which makes a depression probability out of my typing speed, does this seemingly harmless datum become a health datum. (91T)
Discrimination	categorical treatment of a person and an associated negative evaluation [1, p. 295]	9	7	general	Data Collection & Storage	Legal Framework, Informational Power	To differentiate between groups (and individuals) some form of discrimination is necessary. This can be done by using collected information about data subjects. The differentiation is more precise the more (varied) information about the data subject is available.	When assessing credit worthiness, scoring companies use various kinds of information to distinguish credit-worthy applicants from others. In 2022, Equifax, Australia's biggest credit scoring company, announced it would also use people's postal codes for discriminate applicates into groups of different credit worthiness [12].	I see the causes [of discrimination] first and foremost in the existing social structures of domination. That's where they are created, yes, they reproduce themselves in the digital space and also... That's why they have their origin in the processing, that is, the collection and processing of data. So that's where the real origin is. Yes, it is not the stupidity of users. [...] I'm just saying it because that's how it's often communicated. First and foremost, I see the cause in the data-processing organizations, whether they are state authorities and agencies or companies. And also in the way digital markets are structured and regulated or deregulated. (15T)

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
			2		Emergence of Information		To differentiate between groups (and individuals) some form of discrimination is necessary. In addition to existing data, controllers can also use algorithms to classify data subjects or make predictions that are used as the basis for classification. Newly derived data about a data subject results from both processes. The more (varied) information about data subjects is available, the more options exist for the generation of additional information.	The marketing and personalization company Signal uses data collected about data subjects to infer additional information about them, saving this information into a profile for more precise targeting. A 2022 report with a focus on online gambling listed customer group (e.g. "high value"), customer life stage (e.g. "winback", "grow"), overall customer value score (1-9), or overall customer value band (e.g. "very high value", "low value", "very low value") as some of the values being derived from user data and used to differentiate some customers from others [13].	It can happen that groups and, consequently, individuals are discriminated against. Not even intentionally, but simply by algorithms that address certain clusters of people. And that always means that certain classes of people are not addressed, and certain information is only sent to a specific group and not to another group. Then, in a certain sense, the other group is also discriminated against, especially when it comes to political orientation or religious orientation, for example. That is a very big aspect and a very negative consequence. (98T)
Reidentification	linking de-identified data to outside information with the result of discovering the true identity of the data subject the de-identified data relates to adapted from [14]	6	6	general	Data Combination	Unique IDs (08, 23)	Data from various sources can be matched probabilistically and deterministically [15]. Probabilistic matching involves calculating a likelihood of two data sets originating from the same data subject based on shared attributes in these data sets and then combining data sets with a high enough likelihood. Deterministic matching involves using unique identifiers which are the same between data sets to combine them.	The authors of a 2007 paper were able to identify specific imdb Users within a data set of anonymized movie ratings of 500,000 Netflix subscribers by cross-referencing some of the movies the data subjects had also rated on imdb [16].	Combination of identities, so that one practically uses two separate platforms, but then the two platforms suddenly know that this is the same person. That would be a classic. The opposite of that is that I can practically have several identities, and nobody notices that. [...] So there is a particularly intensive possibility of behaviour control, so to speak. We practically have the change that the web is more about individualisation and about clearly holding on to identities. You experience this in everyday life when you use single sign-on on platforms to move forward faster. Conversely, there are the advertising IDs. That means, my surfing behaviour can be tracked between different computers and you get a relatively good idea of what I'm up to, even if I delete the cookies. By linking identities, behaviour becomes much easier for third parties to analyze and third parties know more about you than you do. That would be the risk. (23T)
Identity Theft	acquisition of personal data or documents by an attacker who uses this information to pass themselves off as the victim	6	6	general	Permanence of Information, Data Disclosure	Security	The identity thief can get access to data through a variety of ways (for example through data breaches or a leaks) and can use this data for a various purposes such as to pose as another person when apprehended for a crime (criminal identity theft), to obtain credit, goods, and services (financial identity theft), to assume their identity in daily life	According to the Identity Theft Resource Center, the year 2021 saw a record number of 1,862 unauthorized access, acquisition or disclosure of data with a variety of causes (like Cyberattacks, Human or System Errors, or Physical Attacks) [17] some of which can be guarded against by Security measures.	Then the privacy risks - so that the data is going to be used to basically intrude upon my personal life in a way that I haven't signed up for. And I would drop into some of the bad actor type of risks, of privacy intrusion from other people - so, you know, I can share some data with people who I thought I trusted and then they pissed me off - or the data gets lost and some

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
							(identity cloning), or to obtain medical care or drugs (medical identity theft).		other people send me a lot of spam stuff and then within that, then we link into disruption of other data and other services. You know, your viruses and your bots and the rest of that kind of stuff, because if you share some data, then you've opened up a portal into those sorts of issues. Then identity issues. So people using my identity or aspects of my identity to do things either in my name or using my details that I wouldn't want to happen (74)
Defectiveness of Information	inaccuracy of personal information [1, p. 305]	4	4	general	Data Collection & Storage, Emergence of Information	Data Rectification, Data Erasure	Newly collected or inferred information can also be wrong du to measuring errors, purposeful obfuscation, or inadequate models for inference.	In Detroit, a man was falsely arrested for theft because the facial recognition software identified him from the surveillance tapes [18].	So, one basic example that we have, let's say that Google marks me as a person who really enjoys steak restaurants and that I'm classified as a meat eater, but what if I decide today that from today on I'm going to be vegetarian, right? Then I still get suggestions and recommendations about meat products, although this is no longer relevant. (96)
Permanence of Information	adverse effects that result from the long-term availability of information, influenced by factors such as digitization, storage capacity, decentralization and redundancy of storage on the internet. adapted from [1, p. 299]	3	3	general	Data Storage	Data Erasure	Digital data storage comes with long term accessibility as well as ease of copying, which in the worst case limits individual control over the use of one's own data	A man in Spain had to sue Google to get a link to a digitized 1998 newspaper article about an auction for his foreclosed home deleted. This article would show up, whenever one googled the man's name even though the debt the foreclosure was based on had subsequently been paid [19].	A possible negative consequence of data processing as a whole is that these data no longer disappear. So the fact that data can be copied, that data has different storage locations, is a possible negative consequence. And the more storage locations there are for the data, the more difficult it is to delete. (81T)

Note: Context specifications are provided in Table XI.

TABLE X

TANGIBLE CONSEQUENCES

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
Loss of Privacy	perceived violation of existing (contextual) informational norms, sometimes connected with a perceived loss of control	22	12	general	Data Collection & Storage, Data Disclosure	Tracking, Permanence of Information, Access Control	In the context of big data, data subjects are tracked on desktop, mobile [20] and across devices [21] - often without being aware of such practices and of the data generated about them. This constitutes a violation of privacy norms as their perception of the context (esp. w.r.t. the types of data transmitted and the number of recipients) is different to the actual collection and disclosure of data. This is reflected in the users' perceived loss of privacy [22]. Also, the storage of such data outside the data subject's influence facilitates its copying which additionally limits individual control over the use of one's own data and increases the likelihood of privacy norms being violated.	In a 2017 study, researchers browsed 100 popular sites with two different virtual devices, identifying third parties that received data as well as the data they received [21]. They found that (1) 861 third-party domains collected data on both virtual devices, that could be used for probabilistic device linkage; (2) at least 16 out of the 100 sites shared personally identifiable information with third parties, which could allow them parties to correlate multiple devices to persistent real world identifiers; (3) 106 third-party domains shared unique, browser-specific cookie identifiers with 210 other third parties, potentially enabling third party tracking companies to share device graph information with each other.	So a big problem, which one can't do much about, are all the tracking things: that you can give a Facebook Like everywhere or share things directly on Facebook, it's just... Facebook gets to know everything you do. They are not the only ones. But there's not much you can do about it... (10T)
			11		Emergence of Information		If new data about the data subject is inferred based on previously collected information, this can be regarded as a breach of contextual integrity dependent on existing informational norms that tolerate inference or norms about what kinds of data should be inferred. Thus, a loss of privacy occurs, when information is inferred that the data subject had not intended to be part of the information flow.	Using data about connections to other people on social networks, studies have been able to relatively precisely predict the user's spouse or romantic partner [23] or if a user is homosexual [24].	For example, these FitBit devices produce so much data and people just give it away, right? Entire series of data and what can be derived from them... Yes, and then there is suddenly absolute horror when they realize what can actually be derived from it and what it can be used for. (30T)
			2	work	Data Collection & Storage		Data collection about employees' activities enables employers to carry out comprehensive surveillance that can result in a perceived lack of privacy.	An employee of a business software company in Texas had their pay reduced based on her keyboard activity, as well a screenshot of whatever she was working photos of her and her work, taken every 10 minutes [25].	What I'm also thinking about is maybe surveillance. And this again, maybe is related to, again, to use of data and unforeseen manners. And I think that today we're seeing this very, very well with the whole technologies used around Covid-19 but in general, any kind of data processing that then can be used for state

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
									surveillance, also your company can surveil you, can control you especially now with so many people working from home and where there are so many technologies that can check whether you're at the desk or not. (51)
Financial Losses	loss of money or access to financial resources	23	3	general	Identity Theft	Publicity Damages	If information that can cause publicity damages is accessed my malicious actors, they can extort their victims by threatening to release that information demanding payment to keep the information private and avert publicity damage.	Users of the adultery website Ashley Madison were targets of extortion after the service was hacked. One blackmailer asked for $230 for them to not share the information with the victim's friends, family and employers [26].	Any kind of extortion or blackmailing that can be made against you because some of your data is accessed whatever it is - whether it's true or is not true, but it can be anything - it can be pictures, it can be... I don't know how you spend your money. Whatever that someone else shouldn't know, maybe in your family or maybe your employer. (51)
			15	financial	Stigmatisation		Based on different kinds of their personal information, data subjects can be excluded from access to financial resources like loans or insurances, resulting in financial losses. In these scenarios, the entity governing access to financial resources profits from information about a variety of people with varying personal information to more precisely assess if the specific data subject should receive access to financial resources, thereby profiting from information asymmetry between the data subject and the controller.	In 2010, in the US minority-owned firms were much less likely to be approved for small business loans than white-owned firms [27], and more likely to receive less money with higher interest rates. This was related to a variety of aspects, such as lower amounts of capital or a poor or small credit histories.	The negative consequences are all kinds of ratings: a credit score, which products are offered at all, where are you included at all? Where do you fall out of the selection process? [...] Or, for example, in the case of loans, where you get a loan or not, which depends more on your living environment than on your disposable income. (18T)
			8		Discrimination		Based on different kinds of their personal information, data subjects can receive differential treatment from access to financial resources like loans or insurances. In these scenarios, the entity administering differential treatment profits from information about a variety of people with varying personal information in order to more precisely assess how the specific data subject should be treated, thereby profiting from information asymmetry between the data subject and the controller.	A 2017 analysis of some major car insurers in four US states showed, that some minority neighbourhoods were charged as much as 30 percent more than other areas with similar accident costs [28].	Then, of course, there are also, let's say, more sensitive applications such as in insurance law. [...] If certain categories of users - perhaps even for reasons they cannot influence, i.e. characteristics they cannot manipulate - are priced lower or pay higher premiums, for example, then there is a threat of discrimination that is probably socially undesirable, but which may be illegal. (03T)

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
			6		Identity Theft		Through various means (such as physical theft, data breaches or phishing emails) an attacker can get into possession of credit card or other payment information and use them to pose as the data subject for the purpose of obtaining goods or services or transferring the data subject's money to accounts linked to the criminal.	In 2021, a man in Liverpool, UK used data relating to more than compromised 1,000 credit cards to book flights and hotels. He also resold the card data as well as discounted goods and holidays that he had purchased using the stolen credit card information [29].	Yes, financially, sure data theft simply in the form of account hacking, orders and so on. (79T)
			5		Manipulation	Legal Framework	Personal data can be used to influence purchasing decisions by presenting specific adverts in specific situations.	In 2019, an advert by an online casino was banned as it was targeted towards people that had googled ways to prevent themselves from betting, offering them free spins in the online casino [30].	It can be manipulation of purchasing decisions. Manipulation is a harsh word, but it's the final consequence. If you look at companies analyzing at what times women feel the ugliest, in order to then be able to play them advertisements for make-up or when teenagers feel the worst and so on, so that they can exploit vulnerable situations. (32T)
Stigmatisation	attribution of characteristics to a person that forms the basis for avoiding or excluding them [1, p. 299]	17	12	general	Discrimination	Defectiveness of Information, ADM	If personal data is used to discriminate some people from others (by assigning them to specific groups), this assumed group membership can serve as the basis on which these people are excluded from various aspects of society.	Facebook allowed advertisers to not show (housing adverts) to people based on their race [31].	The influence of data processing in big data applications or the training of algorithms with this information, which may then also lead to either the data subject or third parties being assigned to certain groups - whereby the assignment itself, in my opinion, is personalization, but which is then no longer considered personal data processing - can then have certain consequences, such as geo-blocking or credit guarantees based on address data or user behavior. (13T)
			2		Publicity Damages		When data one would like to keep private becomes public [publicity damages], this can lead to various forms of exclusion [stigmatization]. The internet can play a reinforcing factor by facilitating the distribution of the stigmatizing information.	A thirteen year old girl was bullied after a topless picture of her was distributed without her knowledge or consent [32]. There also was a hate website against her. She committed suicide as a result.	Private, social disadvantages [...] - I stupidly uploaded my nude photo or sent it to my boyfriend/girlfriend and then I receive hate texts or something like that. Yes, that could also have certain social disadvantages. (61T)
			9	work	Discrimination	Defectiveness of Information, ADM	Data are collected that reveal relevant information that may serve as a basis for exclusion from working opportunities. If automated decisions about	In 2019, the Austrian employment agency rolled out an algorithm that assigned job seekers into one of three categories: people with no need of help, people who might benefit from retraining, and people deemed unemployable. Women and disabled	When I think about a labour market system, what comes to mind is of course what was discussed in Austria, where people are simply restricted in their freedom of occupation.... Where people don't get further

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
							people's career possibilities are made based on personal data, they can result in the exclusion of people from working opportunities.	people were much more likely to be assigned in the lower groups and thus potentially be denied job opportunities [33]. In Virginia, USA, a teacher was fired from her position because a statistical tool used to measure her contribution to her students' test results rated her "value added" to the classroom as too low and outweighed her otherwise positive contributions [34].	training because the algorithm says: "Nope". (36T)
Psychological harm	injury or damage to the psychological health of people adapted from [35]	11	5	general	Loss of Privacy, Informational Power		Privacy problems associated with state surveillance or other aggressive data gathering can create an atmosphere of “risk” and self-censorship effectively deterring people from exercising their rights.	A 2017 study suggests that people are much less likley to engage in a range of online activities online, limiting their expression, being less likely to engage with social media, and more cautious when using search, when made aware of online surveillance by the government [36]. Notably, fewer people respond in that way when being made aware of corporate surveillance. Government and corporate surveillance are not necessarily separate however but oftentimes intertwined - as is the case in the US [37] and China [38].	That's why I would perhaps include psychological consequences instead of physical consequences. And probably not so much because of the concrete data processing, but rather because I can't estimate what will happen. So from this pure fear of having lost control - I could imagine that in one situation or another, this is the greatest risk that can arise. (61T)
			3		Manipulation		Manipulation through targeted advertising can lead to addiction reinforcement.	Targeted Advertising can be used to identify and target alcohol-dependent people that feel a stronger urge to drink alcohol when confronted with alcohol-related cues [39].	It can also have an effect on my health if the data that is processed leads to the conclusion that I am an alcoholic and I still, or precisely because of this, receive a lot of advertising for alcohol then this also has an effect on my health. (21T)
			2		Publicity Damages, Stigmatisation		When data, one would like to keep private, becomes public, this can have significant psychological effects, often amplified through social stigma. The internet can play a reinforcing factor by facilitating the distribution of the stigmatizing information.	A thirteen year old girl committed suicide after being bullied because a topless picture of her had been distributed without her knowledge or consent [32].	So, there is persecution on the opinion level, so to speak, in the sense that when certain things become public, it can relatively quickly turn into a witch hunt on the Internet - also in the press, but the Internet is much faster in this regard... (76T)
			3	health	Loss of Privacy	Health (genomic) data	Privacy concerns can lead to stress for the people affected.	A 2021 study shows that mobile social media privacy concerns are positively related to perceived stress [40].	I'm also thinking because of the specific topic where I work now, which is genomic data, that's a risk of personal data processing - even when it's made in the most ethical manner, the most user-central manner - when you process health data, and genomic data specifically, you as a data subject, you can also reveal some information about yourself or

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
									about your family that you didn't know and you didn't want to know. There are many. Of course, you can learn that your father is not your biological father or your brother or whatever, your son [laughs] - and so there are many different ways of putting it. You can also learn that you're going to develop certain illnesses until like a point in time which scares you and gives you anxiety. So let's say there is a more psychological effect today about something that you learn. (51)
Manipulation*	imposing a hidden or covert influence on another person's decision-making [41]	8	8	general	Discrimination		Being able to accurately discriminate between groups or individuals allows for communications to be more precisely tailored to influence the decision-making of said persons, e.g. by taking into account their values, specific issues important to them, their emotional state or other background information to determine content and timing of the communication.	In 2019, in an online call to action the UK's conservative party asked people to provide their personal data as well information on their previous voting behavior and the most "important issue" to them and their families. The associated privacy policy stated that this information (in combination with other commercially available data) would be used to "to determine whether or not to send a voter campaign materials and, if so, to tailor the messages contained within it" [42]. A 2019 report by the Oxford Internet Institute found that such and other techniques of organized social media manipulation were used by 70 countries to manipulate public opinion [43].	People often talk about the existence of vulnerable consumers. In my opinion, this is not correct, because every consumer is vulnerable. However, everyone is vulnerable in different situations. One is an expert in one area and another in another. But everyone has a weak spot somewhere, and many procedures are aimed precisely at finding these weak spots and then exploiting them in a targeted manner. I think that is a great danger. The same applies, of course, to influencing electoral decisions, for example. But at the end of the day, I would say that it is often irrelevant, at least in terms of the technology that is used, whether it is advertising for elections or advertising for products. It is always the case that attempts are made to find certain trigger points in the people concerned who are usually unaware of it and this is precisely how this asymmetry arises. (32T)
Publicity damages	harms occurring without additional circumstances outside the person concerned - i.e. already with the publicity of the information [1, p. 294]	7	3	general	Decontextualization	Defectiveness of Information	When (possibly false) personal information is shared with recipients it was not meant for, this can result in reputational damage.	When sexually explicit images are shared with different people than originally intended, this may impact the reputation [44] and cause shame and embarrassment. Convolutional Neural Networks also allow for the creation of such material without the depicted ever having to take the images [45].	Social aspects in any case. Behavioural predictions can be made that could lead to me possibly being put in jail, which is much more conceivable in the U.S. than in Germany, but nevertheless, taken to the extreme, there are of course such consequences of a social nature, because perhaps when certain data evaluations are made, this has an impact on the perception of me among my friends et cetera or in the family. (21T)

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
			3		Identity Theft		Identity thieves claiming to be other people can cause enormous social damage by engaging in behaviour frowned upon by the social circle of their victims.	People whose identities are stolen face social stigma, after the accounts impersonating them distribute pornography or share NFT recommendations[46].	Loss of identity can mean that they are almost uprooted from society because we are all now - or many of us are - very much involved in these digital communities. Whoever takes over the identity can completely discredit them, they can put you down in all the user groups that they are connected to. So this goes far beyond just financial damage. I don't even know exactly how the penal code actually defines these offenses which identity theft entails. So some of it might be taken up by bullying et cetera and so on. But this certainly is not everything that can result from identity theft. (07T)
			7	work	Decontextualization		When information is decontextualized and received by people not included in the originally intended set of recipients, it can be the cause of reputational damage. This may be the case for workplace information being disclosed outside the workplace but also for information not meant for the workplace to be disclosed to co-workers.	A woman called her boss an idiot and incompetent in his role on Facebook which eventually resulted in disciplinary proceedings for gross misconduct at her workplace [47].	And professionally, it is often a loss of reputation when you share things that are not relevant for others or when things are shared consciously or unconsciously and then really spread. That also means sometimes unconsciously, by email or other media channels. (79T)
Physical harm	injury or damage to the physical health of people adapted from [35]	5	3	general	Manipulation		Manipulation through targeted advertising can lead to addiction reinforcement.	Targeted Advertising can be used to identify and target alcohol-dependent people that feel a stronger urge to drink alcohol when confronted with alcohol-related cues [39].	It can also have an effect on my health if the data that is processed leads to the conclusion that I am an alcoholic and I still, or precisely because of this, receive a lot of advertising for alcohol then this also has an effect on my health. (21T)
			2	health	Defectiveness of Information	ADM	Due to incorrect data and automatic/opaque decisions, incorrect medical treatment/medication errors may occur.	Relying on algorithms for decision making has lead to reduced service hours for people with physical disabilities [48] and the black patients being assigned a lower priority for the treatment of complex conditions [49], including diabetes and kidney problems which can lead to an exacerbation of their health problems. Making decisions based on uncomplete or wrong information can also endanger the data subject, such as giving penicillin, without having the correct information about the patient's	Take the example of me going to the doctor and my personal data is not correct and then I get the wrong treatment or something like that. (32T)

Consequence	Definition	N	n	Context	Causes	Potential Modulators	Explanation	Example	Quote
								allergies [50] which can result in an anaphylactic shock (maximal allergic reaction) which is potentially fatal.	

Note: Context specifications are provided in Table XI.

TABLE XI
CONTEXT SPECIFICATION

Context	Actors	Data Types	Purposes
Financial	Usually hold financial resources which are transferred between actors	Usually payment information	Any kind of financial transaction, usually transfer of financial resources in exchange of good or services
Health	Person receiving medical treatment and medical personnel or insurance	Health information	Administration of medical treatment or for medical diagnosis
Work	(Potential) employee and employer	Various, including information found on a résumé or performance information	Various, including recruitment or management

REFERENCES

[1] S. Drackert, *Die Risiken der Verarbeitung personenbezogener Daten: eine Untersuchung zu den Grundlagen des Datenschutzrechts*. Freiburg im Breisgau, Germany: Duncker & Humblot, 2014.

[2] R. Calo and A. Rosenblat, "The Taking Economy: Uber, Information, and Power" *Columbia Law Review*, vol. 117, no. 6, 2017. [Online]. Available: https://columbialawreview.org/content/the-taking-economy-uber-information-and-power/

[3] D. Davidson, 'Facebook targets "insecure" young people to sell ads,' *The Australian*, May 01, 2017. [Online]. Available: https://web.archive.org/web/20220721133333/https:/www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

[4] G. J. X. Dance, M. LaForgia, and N. Confessore, "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants," *New York Times*, Dec. 18, 2018. [Online]. Available: https://web.archive.org/web/20220816051401/https:/www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

[5] R. Morgan, 'Uber settles federal probe over "God View" spy software,' *New York Post*, Aug. 15, 2017. [Online]. Available: https://web.archive.org/web/20170830041641/https://nypost.com/2017/08/15/uber-settles-federal-probe-over-god-view-spy-software/.

[6] noyb, 'NCC & noyb GDPR complaint: "Grindr" fined € 6.3 Mio over illegal data sharing,' *noyb.eu*, Dec. 15, 2021. [Online]. Available: https://web.archive.org/web/20220809113416/https:/noyb.eu/en/ncc-noyb-gdpr-complaint-grindr-fined-eu-63-mio-over-illegal-data-sharing.

[7] B. Tau and G. Wells, “Grindr User Data Was Sold Through Ad Networks,” *The Wall Street Journal*, May 02, 2022. [Online]. Available: https://web.archive.org/web/20220510144107/https:/www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800.

[8] J. L. Kröger, O. H.-M. Lutz, and F. Müller, “What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking” in *Privacy and Identity Management. Data for Better Living: AI and Privacy*, M. Friedewald, M. Önen, E. Lievens, S. Krenn, and S. Fricker, Eds. in IFIP Advances in Information and Communication Technology, vol. 576. Cham: Springer International Publishing, 2020, pp. 226–241. [Online]. doi: 10.1007/978-3-030-42504-3_15.

[9] J. L. Kröger, O. H.-M. Lutz, and P. Raschke, “Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference”, in *Privacy and Identity Management. Data for Better Living: AI and Privacy*, M. Friedewald, M. Önen, E. Lievens, S. Krenn, and S. Fricker, Eds., in IFIP Advances in Information and Communication Technology, vol. 576. Cham, Switzerland: Springer International Publishing, 2020, pp. 242–258. [Online]. doi: 10.1007/978-3-030-42504-3_16.

[10] J. L. Kröger, P. Raschke, and T. R. Bhuiyan, “Privacy implications of accelerometer data: a review of possible inferences” in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, Jan. 2019, pp. 81–87. [Online]. doi: 10.1145/3309074.3309076.

[11] N. Grant, “Google Says It Will Delete Location Data When Users Visit Abortion Clinics,” *New York Times*, Jun. 01, 2022. [Online]. Available: https://web.archive.org/web/20220814163925/https:/www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html.

[12] D. Ziffer, ‘Threat of “postcode discrimination” as credit scores skewed by where you live,’ *ABCNews*, Feb. 06, 2022. [Online]. Available: https://web.archive.org/web/20220804080606/https:/www.abc.net.au/news/2022-02-07/threat-of-postcode-discrimination-in-credit-scores/100723574.

[13] W. Christl. Digital Profiling In the Online Gambling Industry, Jan. 2022. [Online]. Available: https://web.archive.org/web/20220620085332/https:/cdn.sanity.io/files/btrsclf0/production/e23ea75fe93f775d9f9ed795427f4b5ed8d67016.pdf.

[14] P. Ohm, “Broken promises of privacy: Responding to the surprising failure of anonymization” *UCLA Law Review*, vol. 57, 2009, pp. 1701-1777. [Online]. Available: https://www.uclalawreview.org/broken-promises-of-privacy-responding-to-the-surprising-failure-of-anonymization-2/

[15] O. Binette and R. C. Steorts, “(Almost) all of entity resolution” *Sci. Adv.*, vol. 8, no. 12, Mar. 2022, p. eabi8021. [Online]. doi: 10.1126/sciadv.abi8021.

[16] A. Narayanan and V. Shmatikov. How To Break Anonymity of the Netflix Prize Dataset, Nov. 2007. [Online]. Available: http://arxiv.org/abs/cs/0610105.

[17] Identity Theft Resource Center. Data Breach Annual Report, Jan. 2022. [Online]. Available: https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf.

[18] B. Allyn, '"The Computer Got It Wrong": How Facial Recognition Led To False Arrest Of Black Man,' *National Public Radio*, Jun. 24, 2020. [Online]. Available: https://web.archive.org/web/20220823155355/https:/text.npr.org/882683463.

[19] J. Powles, 'What we can salvage from "right to be forgotten" ruling,' *Wired UK*, May 15, 2014. [Online]. Available: https://web.archive.org/web/20140516024112/http:/www.wired.co.uk/news/archive/2014-05/15/google-vs-spain.

[20] Z. Yang and C. Yue, "A Comparative Measurement Study of Web Tracking on Mobile and Desktop Environments" in *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, Apr. 2020, pp. 24–44. [Online]. doi: 10.2478/popets-2020-0016.

[21] J. Brookman, P. Rouge, A. Alva, and C. Yeung, "Cross-Device Tracking: Measurement and Disclosures" in *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 2, Apr. 2017, pp. 133–148. [Online]. doi: 10.1515/popets-2017-0020.

[22] W. Thode, J. Griesbaum, and T. Mandl, '"I Would Have Never Allowed It": User Perception Of Third-Party Tracking And Implications For Display Advertising' in *Proceedings of the 14th International Symposium on Information Science (ISI 2015)*, May 2015, pp. 445-456. [Online]. doi: 10.5281/ZENODO.17971.

[23] L. Backstrom and J. Kleinberg, "Romantic partnerships and the dispersion of social ties: a network analysis of relationship status on facebook" in *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, Feb. 2014, pp. 831–841. [Online]. doi: 10.1145/2531602.2531642.

[24] C. Jernigan and B. F. T. Mistree, "Gaydar: Facebook friendships expose sexual orientation," *FM*, Sep. 2009. [Online]. doi: 10.5210/fm.v14i10.2611.

[25] M. Barbaro, "The Rise of Workplace Surveillance," *New York Times*, Aug. 24, 2022. [Online]. Available: https://www.nytimes.com/2022/08/24/podcasts/the-daily/workplace-surveillance-productivity-tracking.html.

[26] K. Rogers, "After Ashley Madison Hack, Police in Toronto Detail a Global Fallout," *New York Times*, Aug. 24, 2015. [Online]. Available: https://web.archive.org/web/20210525041846/https:/www.nytimes.com/2015/08/25/technology/after-ashley-madison-hack-police-in-toronto-detail-a-global-fallout.html.

[27] R. W. Fairlie, A. M. Robb, and D. Hinson, Disparities in Capital Access Between Minority and Non-minority-owned Businesses. US Department of Commerce, Minority Business

Development Agency, 2010. [Online]. Available: https://www.mbda.gov/sites/default/files/migrated/files-attachments/DisparitiesinCapitalAccessReport.pdf

[28] J. Angwin, J. Larson, L. Kirchner, and S. Mattu, "Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk," *ProPublica*, Apr. 05, 2017. [Online]. Available: https://web.archive.org/web/20220823135256/https:/www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk.

[29] A. Weston, "Nan of 11 helped Scouse fraudster launder dirty cash," *Liverpool Echo*, Jun. 24, 2021. [Online]. Available: https://web.archive.org/web/20210727092948/https:/www.liverpoolecho.co.uk/news/liverpool-news/nan-11-helped-scouse-fraudster-20894839.

[30] Davies, "Online casino advert banned for targeting problem gamblers," *The Guardian*, Oct. 09, 2019. [Online]. Available: https://web.archive.org/web/20220222234321/https:/www.theguardian.com/society/2019/oct/09/casumo-ad-banned-for-targeting-people-trying-to-stop-gambling.

[31] J. Angwin, A. Tobin, and M. Varner, "Facebook (Still) Letting Housing Advertisers Exclude Users by Race," *ProPublica*, Nov. 21, 2017. [Online]. Available: https://web.archive.org/web/20220818050403/https:/www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

[32] R. Kaye, "How a cell phone picture led to girl's suicide," *CNN*, Oct. 07, 2010. [Online]. Available: https://web.archive.org/web/20220802154657/https:/edition.cnn.com/2010/LIVING/10/07/hope.witsells.story/index.html.

[33] N. Kayser-Bril, "Austria's employment agency rolls out discriminatory algorithm, sees no problem," *AlgorithmWatch*, Oct. 06, 2019. [Online]. Available: https://web.archive.org/web/20220326073035/https:/algorithmwatch.org/en/austrias-employment-agency-ams-rolls-out-discriminatory-algorithm.

[34] B. Turque, '"Creative ... motivating" and fired,' *The Washington Post*, Mar. 06, 2012. [Online]. Available: https://web.archive.org/web/20220523031452/https:/www.washingtonpost.com/local/education/creative--motivating-and-fired/2012/02/04/gIQAwzZpvR_story.html.

[35] ISO. ISO/IEC Guide 51:201. [Online]. Available: https://www.iso.org/standard/53940.html.

[36] J. W. Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study" *Internet Policy Review*, vol. 6, no. 2, May 2017, pp. 1-39. [Online]. doi: 10.14763/2017.2.692.

[37] G. Greenwald and E. MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian*, Jun. 07, 2013. [Online]. Available:

https://web.archive.org/web/20220819195233/https:/www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[38] S. Ikeda, "China's New Data Protection Law Maintains Full State Access To Private Information, but Puts Clamps on Tech Firms Comparable to EU's GDPR," *CPO Magazine*, Aug. 24, 2021. [Online]. Available: https://web.archive.org/web/20211027030825/https:/www.cpomagazine.com/data-protection/chinas-new-data-protection-law-maintains-full-state-access-to-private-information-but-puts-clamps-on-tech-firms-comparable-to-eus-gdpr/.

[39] World Health Organization, WHO highlights glaring gaps in regulation of alcohol marketing across borders, May 2022. [Online]. Available: https://web.archive.org/web/20220706044808/https:/www.who.int/news/item/10-05-2022-who-highlights-glaring-gaps-in-regulation-of-alcohol-marketing-across-borders.

[40] A. Stevic *et al.*, "Privacy concerns can stress you out: Investigating the reciprocal relationship between mobile social media privacy concerns and perceived stress" *Communications*, vol. 47, no. 3, Sep. 2022, pp. 327–349. [Online]. doi: 10.1515/commun-2020-0037.

[41] D. Susser, B. Roessler, and H. Nissenbaum, "Technology, autonomy, and manipulation" *Internet Policy Review*, vol. 8, no. 2, Jun. 2019, pp. 1-22. [Online]. doi: 10.14763/2019.2.1410.

[42] N. Lomas, "UK watchdog eyeing PM Boris Johnson's Facebook ads data grab," *TechCrunch*, Aug. 05, 2019. [Online]. Available: https://web.archive.org/web/20210331195317/https:/techcrunch.com/2019/08/05/uk-watchdog-eyeing-pm-boris-johnsons-facebook-ads-data-grab/.

[43] S. Bradshaw and P. N. Howard. The global disinformation order: 2019 global inventory of organised social media manipulation, Sep. 2019. [Online]. Available: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

[44] E. Gray, "Adult Sexting: Does It Help Or Hurt Relationships?," *The Huffington Post*, Apr. 20, 2012. [Online]. Available: https://web.archive.org/web/20220705162850/https:/www.huffpost.com/entry/adult-sexting-relationships_n_1439404).

[45] J. Vincent, "New AI deepfake app creates nude images of women in seconds," *The Verge*, Jun. 27, 2019. [Online]. Available: https://web.archive.org/web/20220812062103/https:/www.theverge.com/2019/6/27/18760896/deepfake-nude-ai-app-women-deepnude-non-consensual-pornography.

[46] P. R. Allison, "Attack of the clones: the rise of identity theft on social media," *ComputerWeekly.com*, May 31, 2022. [Online]. Available: https://web.archive.org/web/20220717223131/https:/www.computerweekly.com/feature/Attack-of-the-clones-the-rise-of-identity-theft-on-social-media.

[47] S. Hashmy-Elsby, “Think before you overshare. Yes, it can get you fired,” *BBC*, Aug. 27, 2016. [Online]. Available: https://web.archive.org/web/20190914131818/https://www.bbc.com/worklife/article/20160826-think-before-you-overshare-yes-it-can-get-you-fired.

[48] C. Lercher, “A healthcare algorithm started cutting care, and no one knew why,” *The Verge*, Mar. 21, 2018. [Online]. Available: https://web.archive.org/web/20220712190512/https:/www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy.

[49] Z. Obermeyer, B. Powers, C. Vogeli, and S. Mullainathan, “Dissecting racial bias in an algorithm used to manage the health of populations” *Science*, vol. 366, no. 6464, Oct. 2019, pp. 447–453. [Online]. doi: 10.1126/science.aax2342.

[50] J. K. Aronson, “Medication errors: what they are, how they happen, and how to avoid them”, *QJM*, vol. 102, no. 8, Aug. 2009, pp. 513–521. [Online]. doi: 10.1093/qjmed/hcp052.