



Best practices and current implementation of emerging smartphone-based (bio)sensors – Part 1: Data handling and ethics



G.M.S. Ross ^{a, b, 1}, Y. Zhao ^{c, 1}, A.J. Bosman ^{a, b}, A. Geballa-Koukoulou ^a, H. Zhou ^d, C.T. Elliott ^{e, f}, M.W.F. Nielen ^{a, b}, K. Rafferty ^{c, 2}, G.IJ. Salentijn ^{a, b, 2, *}

^a Wageningen Food Safety Research (WFSR), Wageningen University & Research, P.O. Box 230, Wageningen, 6700 AE, the Netherlands

^b Laboratory of Organic Chemistry, Wageningen University, Stippeneng 4, Wageningen, 6708 WE, the Netherlands

^c School of Electronics, Electrical Engineering & Computer Science, Queen's University Belfast, 16A Malone Road, Belfast, BT9 5BN, United Kingdom

^d School of Computing and Mathematical Sciences, University of Leicester, University Road, Leicester, LE1 7RH, United Kingdom

^e Institute for Global Food Security, School of Biological Science, Queen's University Belfast, 19 Chlorine Gardens, Belfast, BT9 5DL, United Kingdom

^f School of Food Science and Technology, Faculty of Science and Technology, Thammasat University, 99 Mhu 18, Phahonyothin road, Khong Luang, Pathum Thani, 12120, Thailand

ARTICLE INFO

Article history:

Received 30 September 2022

Received in revised form

24 November 2022

Accepted 25 November 2022

Available online 1 December 2022

Keywords:

Data acquisition

Data processing

Artificial intelligence

Privacy

Security

GDPR

ABSTRACT

Smartphones are ubiquitous in modern society; in 2021, the number of active subscriptions surpassed 6 billion. These devices have become more than a means of communication; smartphones are powerful, continuously connected, miniaturized computers capable of passively and actively collecting (private) information for us and from us. Their implementation as detectors or instrumental interfaces in emerging smartphone-based (bio)sensors (SbSs) has facilitated a shift towards portable point-of-care platforms for healthcare and point-of-need systems for food safety, environmental monitoring, and forensic applications. These familiar, handheld devices have the capacity to popularize analytical chemistry by simplifying complicated laboratory protocols and automating advanced data handling without requiring expensive equipment or trained analysts. To elucidate the technological, legal, and ethical challenges associated with developing SbSs, we reviewed the existing literature (2016–2021), providing an in-depth critical analysis of state-of-the-art optical and electrochemical SbSs. This analysis revealed the key areas to consider for emerging SbSs, which we will address in a set of review papers. Part I (this review) will consider (i) how the SbS data are acquired and processed and (ii) the implementation of privacy and data protection strategies to keep this data secure. Part II will then focus on (iii) the development and validation of biosensors and (iv) how to assess the usability and (potential) social impact of emerging SbSs.

Finally, these insights are applied to generate proposed best practices to help guide the future ethical data handling and development of smartphone-based devices for analytical chemistry applications.

© 2022 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Industry 4.0, the amalgamation of smart technologies, is breaking the boundaries between physical, digital, and biochemical disciplines. Industry 4.0 includes artificial intelligence (AI), mobile technologies, cloud computing, 3D-printing, and the Internet of

Things (IoT), a network of interconnected devices with embedded sensors that communicate with each other via the Cloud [1]. The ubiquity of smartphones makes them the foundation of industry 4.0; in 2022, over 6.6 billion people will own a smartphone worldwide [2,3]. Smartphones are essentially handheld computers, and their software applications (i.e., Apps) can passively collect temporal, geographical, screen usage, and other information from an array of embedded sensors, including accelerometers, gyroscopes, barometers, proximity, and pressure sensors. Additionally, their powerful central processing units (CPUs) enable them to actively acquire data using their front-facing cameras [4], rear-facing cameras [5], ambient light sensors (ALS) [6], capacitive

* Corresponding author. Wageningen Food Safety Research (WFSR), Wageningen University & Research, P.O. Box 230, Wageningen 6700 AE, the Netherlands.

E-mail address: gert.salentijn@wur.nl (G.IJ. Salentijn).

¹ co-first author.

² co-corresponding author

touch sensors [7], microphones, and geolocating sensors. See Supplementary Information (SI) Fig. S1 for a graphical representation of these on-device sensors. Moreover, smartphones can wirelessly receive data from externally connected devices that transduce signals into digital information before transmitting the results via Wi-Fi, Bluetooth, or near-field communication (NFC) [8,9]. Likewise, smartphone-connected physical activity (PA) trackers and smartwatches allow consumers to self-monitor several variables related to daily activity and sleep performance. The PA information from these wearables can help individuals learn about themselves, potentially providing a powerful healthcare intervention tool [10,11]. At the same time, connected devices that track the user's location, behavioral patterns, and spending habits present unprecedented security and personal privacy risks.

Besides their widespread use in society, as alluded to above, smartphones have been the subject of many scientific studies exploring their applicability to perform portable (bio)chemical analysis. In this context, smartphones can be standalone devices for collecting and analyzing data, or combined with compact attachments/adapters for specific biosensing applications [12]. Smartphone-based Sensors (SbSs), often using affordable and customizable (3D-printed) parts [13], have emerged as a trend with the potential to popularize analytical chemistry. These familiar, rapid, handheld devices help simplify complicated laboratory protocols without requiring expensive equipment or technical expertise. Portable SbS platforms can enable next-generation personalized healthcare at the point-of-care (PoC) [14], enhance food safety for industry and consumers [15–17], and facilitate real-time monitoring of environmental contaminants at the point-of-need (PoN) [18]. Since 2016, over 50 review articles have been published on electrochemical [19–21] and optical SbSs [22], using labeled colorimetric [23], fluorescence [24], chemiluminescence, bioluminescence, photoluminescence [25], and label-free ALS [6], spectroscopic [3] and plasmonic [26] detection mechanisms. The number and diversity of these reviews affirm the trend in using SbSs for portable analytical applications across healthcare, food safety, environmental monitoring, forensics, and beyond. Moreover, these numerous publications highlight a shift towards enabling consumers to carry out (bio)chemical analysis using their personal smartphones.

A key advantage of SbSs is their ability to collect (approx. 1–5 MB/photo, or 100–600 MB/min of video – depending on the data format and applied quality configuration), analyze (over 1 GHz in clock rate – the running frequency of the CPU [27]), and store (8–512 GB) or transfer (up to approx. 100 megabits per second (Mbps) for 4G mobile networks [28]) large quantities of raw information [29] and to securely transmit the interpreted results to relevant authenticated parties by network encryption protocols [30]. Yet, the complexities associated with SbS data handling related to data collection, processing, interpretation, and storage/persistence, are rarely reported in the literature. Furthermore, despite having the potential to decentralize analytical chemistry, the (mis)use of SbSs poses several risks for end-users and myriad legal and ethical challenges related to handling private, personal data. Here, the number of papers describing smartphone-based *analytical devices*, *optical biosensors*, *electrochemical biosensors*, and *mobile phone biosensors* were plotted per year of publication (Fig. 1A) to elucidate the trend of using SbSs for applications in analytical chemistry. These publications were then further categorized based on specific parameters related to (i) data acquisition and handling and (ii) privacy and data protection (Fig. 1B); these are also the main aspects of SbSs discussed in this review. To this end, a structured keyword search was carried out using predefined inclusion and exclusion criteria. In brief, a keyword search was conducted in the Web of Science, Scopus, and IEEE Explore online

databases. Only peer-reviewed research papers published between 2016 and 2022 were included in this review. After removing duplicates, 886 unique articles were identified by the keyword search (see also Supplementary Information (SI) for more detail).

The first section of this review will provide an in-depth analysis of the state-of-the-art optical and electrochemical SbSs, assessing emerging trends for efficient, authentic analytical data acquisition and handling. The following section of the review will deconstruct privacy and data protection legislations and ethical frameworks related to interfacing smartphones with biosensing devices for data collection. This review (Part I) will finish with perspectives and proposed best practices for advanced data handling and privacy protection for emerging SbSs. Finally, the companion review (Part II) will explore how ethical R&D practices should guide and enable the sustainable design, development, and validation of emerging SbSs and assess the broader impact of such SbSs on consumers allowing for a holistic reflection on their implementation and acceptance in society. Parts I and II of this review series will generate insights that should help to shape the future ethical development and data handling of SbSs for analytical chemistry applications.

2. Acquisition & handling of data from smartphone-based (bio)sensors

Smartphones can acquire signals from connected biosensors, but the raw data from optical measurements or electrochemical information they collect requires further processing before the end user can interpret the test result. The data handling process can be split into four steps, as described in Table 1: (1) data collection, (2) data processing, (3) data interpretation, and (4) data persistence. From an SbS perspective, data collection involves translating the physical [31], chemical [32], or biological [33] properties of a sample into digital, analytical data. Following collection, the analytical data requires processing to minimize any compromising noise (e.g., random noises [34] and dust on the camera lens [35]) and to compensate for the lack of standardized conditions (e.g., variations in background [36], illumination [37], and intrinsic camera properties [38]). Afterwards, the SbS interprets the processed analytical data, on-device, or remotely before presenting it back to the end-user as either qualitative [39], semi-quantitative [40], or quantitative [41] test results. Finally, the collected data and interpreted results are stored in databases (i.e., data persistence), either locally on the smartphone [42] or remotely on a desktop computer [40] or cloud server [33], for data management, future auditing, and (further) analysis.

2.1. Analytical data formats

Currently, the two main categories of SbSs reported in the literature are based on 'optical' (155/886) and 'electrochemical' (104/886) detection (Fig. 1A). Optical detection mechanisms use the smartphone camera or ambient light sensor (ALS) to collect data. In contrast, electrochemical SbSs typically use portable 'plug-in' potentiostats that connect with a smartphone as a power source and computer. Both optical and electrochemical measurements can be susceptible to variation. For electrochemical analysis, these variations can arise from differences in voltage, current, and overall power output as well as differences in electrolyte and reference solutions which can result in increased noise in the measurement [58]. Still, these variations do not arise from the smartphone itself, as it is not the sensing device in electrochemical measurements. In contrast, optical SbS data are highly susceptible to variability during data collection; variations can come from camera differences, the distance at which the photo is recorded, and contaminating

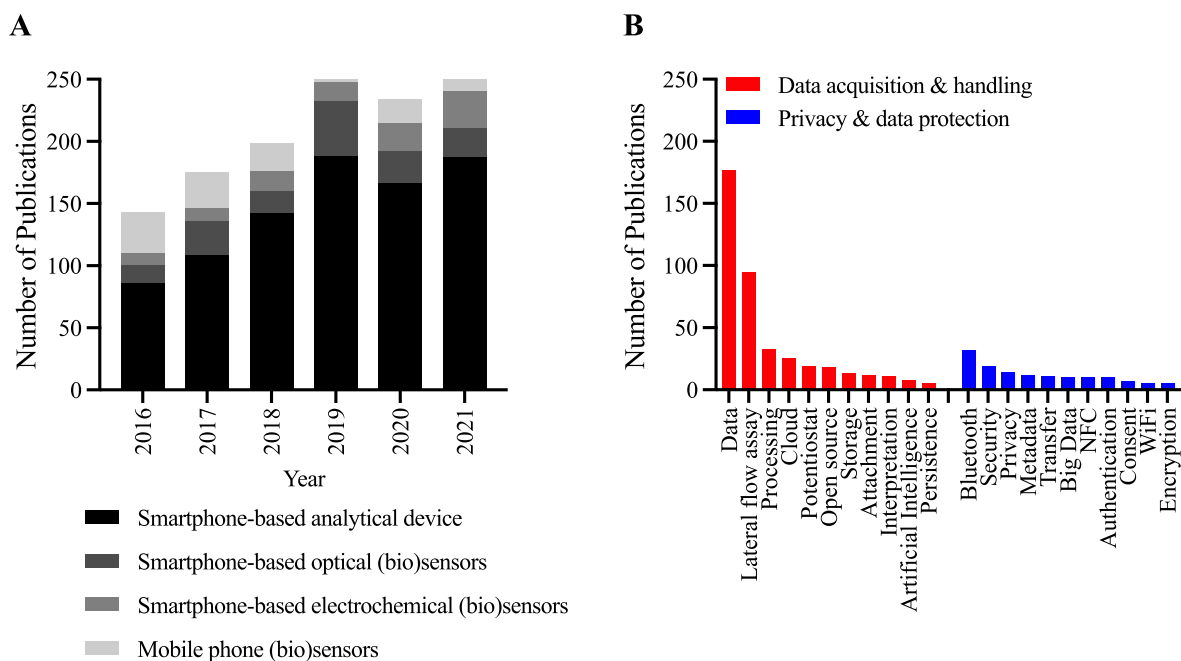


Fig. 1. Overview of the number of publications related to smartphone-based devices, (A) per search term, per year, and (B) per specific keyword.

Table 1
Attributes for data handling in SbSs.

Attributes	Example values
Analytical data formats	R(ed)G(reen)B(lue) image [36], RGB video [32], Raw image & video data [43], luminance [32], potentiometric [44] voltametric [45] amperometric [46], impedimetric [47]
Conditions during data acquisition	Scene background (controlled [48], semi-controlled [49], uncontrolled [31])
Data collection	Smartphone App interfaces (built-in App [49], third-party App [39], custom-developed App [39])
Data processing	Color space transformation, demosaicing [50], denoising [50] calibration [51], illumination and sensor property normalization [51]
Data interpretation	Feature extraction (e.g., wavelength selection by support vector regression (SVR) [39]), regression (e.g., polynomial regression) [52], classification (e.g., principal component analysis-support vector machine (PCA-SVM) [40]), decision fusion (e.g., support vector machine (SVM) [40]), nyquist plot [47] voltammogram [45]
Data persistence	Image gallery [53], local data storage managed by App [52], and in the cloud [54], blockchain [55]
Artificial intelligence (AI)	Machine learning [42], federated learning [56]
Online or offline data handling	Data handling on the cloud (online) [48], data handling on a smartphone (offline) [57]

ambient light, which is why this review focuses mainly on the (advanced) processing of optical data. The literature also reflects this higher complexity; out of 886 articles, 33 specifically focused on 'data processing' (Fig. 1), and of these, 11 focused on optical, and 7 on electrochemical detection, with the remaining 15 concentrating on technical issues related to SbS system architecture and advanced data handling.

2.1.1. Electrochemical data

Electrochemical sensing detects (bio)molecules by converting a chemical (oxidation or reduction) reaction into a (quantifiable) electrochemical signal that is read by a potentiostat. Smartphone-based electrochemical sensors typically use a smartphone to control and/or collect data from a connected potentiostat. Important embodiments of electrochemical SbSs typically rely on techniques such as potentiometry [59], voltammetry [45], amperometry [46], and impedance spectroscopy [60]. After the electrochemical data is transferred from the potentiostat to the smartphone, it is plotted (e.g., in a voltammogram [45], or Nyquist plot [47]), and differences in the shape of the plot reveal characteristics of the (organic or inorganic) analyte, which enable (quantitative) detection [61]. In

smartphone-based electrochemical biosensing, the smartphone thus functions as a portable computer, so the use of the smartphone should not directly influence the data acquisition process. For this reason, the data acquisition process for electrochemical SbSs is not discussed here in detail, and instead, the reader is directed to a dedicated review on PoC electrochemical SbSs [21].

Still, it is interesting to consider how data is transferred from the connected potentiostat to the smartphone, which can be physically (through the data cable, or audio jack) or wirelessly (by Bluetooth, NFC, or Wi-Fi connection). In one study, researchers used smartphone audio channels (physically connected to a potentiostat by the audio jack) to control the potentiostat, and the smartphone microphone to measure the response [47]. One audio channel was used for powering the impedimetric sensor and for setting the potential, and the other audio channel was used to generate the stimulus for the sensor. Still, this approach was limited because the smartphone only supported two audio output channels, but needed to supply 4 signals (power, AC stimulus, DC bias voltage, and a control signal) which required reusing the audio outputs for different functions, limiting its current usability [47]. In another study, a Bluetooth-operated 'universal wireless electrochemical

detector' (UWED) was developed where a smartphone was used as the user interface for setting the experimental parameters, following the result in real-time, and for transmitting the acquired data from the smartphone to the cloud [62]. Moreover, because the UWED wirelessly transfers data via Bluetooth, it is compatible with all modern smartphones [62]. Alternatively, electrochemical SbSs can be developed using commercial potentiostats and software, which can e.g., be connected to the smartphone by Bluetooth (or by data cable to the USB-C port) [63]. In such work, the potentiostat can be controlled by a dedicated companion app, and the user can view the results in real-time as a video on the smartphone screen [63]. Clearly, electrochemical SbSs offer versatile data transfer options. Moreover, these SbSs can be developed as low-cost, open-source devices, or can use commercial components to accelerate their development.

2.1.2. Optical data

Smartphone camera sensors are based on a color filter array (CFA), called the Bayer filter mosaic; when a raw image is captured, the CFA is superimposed on the image sensor, converting pixels in the image to red, green, and blue signals [50]. The resulting raw output contains spatially separated color information about the scene, but before this data is useful, it requires a demosaicing step to reconstruct the data to a RGB image containing full color information at each pixel position [43,50]. Most smartphones automatically apply an image signal processing step to improve image quality; this step comprises demosaicing, color balance adjustments, and sensor noise mitigation (denoising).

Two main formats of optical data were identified in the reviewed literature, namely, (i) RGB (red, green, blue) images [36] and videos [57] acquired by smartphone cameras, and (ii) light intensity [32] measured by the ALS [64]. Both formats of optical data are useful for different applications, indicating that the sensor choice and data type are application-dependent. For instance, ALS can detect light across a wide range of wavelengths (visible to near-infrared spectrum from approximately 350 nm–1000 nm in wavelength) and luminosity intensities (from 0 to 2000 lx), making it useful for spectrophotometry and colorimetry applications [3,65]. In one study, the smartphone ALS was combined with a 3D-printed cuvette holder and a narrow-spectral-bandwidth LED to acquire spectrophotometric measurements of protein assays such as the Bradford assay, providing a low-cost, open-source alternative to commercial spectrophotometers [65]. In another study, an ALS-based SbS was developed for measuring competitive immunoblotting assays. In this approach, the intensity of the light able to penetrate to the ALS was inversely proportional to the number of precipitates in the assay, which could be (semi)quantified on-device by a dedicated App [66]. These studies demonstrate that ALS-based SbSs can provide a more affordable and portable alternative for reading enzyme-linked immunosorbent assays (ELISA) or other microplate-based turbidity assays compared with laboratory-based spectrophotometers.

The primary optical data generated by SbSs are RGB images captured by the smartphone camera. An RGB image is composed of millions of pixels; each pixel quantifies the red, green, and blue light sampled at the corresponding location (together covering the visible spectrum from approximately 400 nm–700 nm) [37]. When many smartphone images are collected (e.g., one per second) and analysed together, these can be used for the real-time monitoring of dynamic processes [67]. Comparatively, an RGB video contains even more data than an image, i.e., up to 60 frames per second (FPS) collected by the smartphone camera [68]. Such RGB video-based data allows for monitoring important assay characteristics, such as assay signal development over time [69,70]. While video data may provide temporal information, acquiring video measurements

will also introduce additional noise to the data (e.g., motion blur), drain the smartphone battery, and require substantially more storage space.

For optical SbS applications, light intensity reveals information about concentration in colorimetric analysis. In contrast, RGB images report spatial and spectral information about the biosensor or sample, and RGB videos can even contain temporal details on assay development. However, aside from small areas/regions of interest (ROIs), smartphone images and videos contain vast amounts of redundant data that do not contribute to the analytical signal [71]; removing this data before further processing is necessary to prevent it from convoluting the signal.

2.1.3. Metadata

Metadata describes the characteristics of certain data; it is data about data. For example, metadata collected by a smartphone may include geo-coordinates produced by the geolocating sensor, device posture information provided by the gyroscope and accelerometer, user interactions provided by touch sensors, and timestamp information. Such metadata can reveal necessary information about a user's lifestyle and therefore presents personal privacy risks. When an SbS generates data, metadata adds descriptors or classifiers to the analytical data, including the information input by users, such as the sample (or matrix) type, sample number, batch number, date, and description. These metadata and control signals can also be collected and transmitted by SbSs as part of the total data package.

2.2. Conditions during data acquisition

The miniaturization of analytical equipment can facilitate on-site/in-field analysis outside of centralized laboratories. However, the data acquisition conditions still require control as they influence the analytical performance of SbS, especially for optical measurements. In addition, different conditions during acquisition may also pose different levels of risk (e.g., inaccurate interpretation of the tests [36] or leaking of personal information) and operational burdens on the end-user. As shown in Fig. 2, the acquisition conditions can be split into three categories: i.e., (i) controlled, (ii) semi-controlled, and (iii) uncontrolled conditions.

One way to control and standardize the conditions under which data is acquired (scene backgrounds) during optical measurements is to use a custom-developed light-shielding attachment to minimize interference from ambient light [32,48,52,73]. To rapidly prototype these attachments, they can be 3Dprinted; 49/886 articles mention '3D printing' in their keywords/abstract, and 18 of these 49 specifically use the technology to develop lightboxes for SbSs. In one example, a modular 3D-printed lightbox was designed that was compatible with several smartphone models [54]. This plug-and-play approach integrated different modules, including (i) a commercial smartphone case, (ii) a customized connection unit to attach the 3D-printed lightbox, (iii) a customized 3D-printed lightbox with a changeable external light source, and (iv) an adapter to support different assay platforms, e.g., microfluidic chips and lateral flow immunoassays (LFIAs) [54]. In another example, a 3D-printed SbS attachment was developed for the multiplex detection of food allergens [74]; the attachment was later reused to acquire RGB videos of LFIAs to differentiate between false-negative results caused by the hook-effect [69]. Finally, the 3D-printed attachment was repurposed again to analyze commercial domoic acid LFIAs [75], showing that carefully designed SbS attachments can be used for different applications and sometimes work with different smartphone models, as long as the device is of a similar size and camera configuration. Another interesting and low-cost (\$0.15) 3D-printed attachment was reported that coupled the



Fig. 2. Overview of three types of scene backgrounds during acquisition, i.e., uncontrolled, semi-controlled, and controlled conditions, with examples for each type. Reprinted with permission from Refs. [39,54,57,67,72].

smartphone's ALS with a microplate for measuring transmitted light intensity in ELISA measurements. The results from the SbS colorimetric reader were consistent with laboratory-based microplate readers, and the attachment is compatible with different smartphone models [76].

As highlighted above, low-cost and customizable attachments can convert conventional smartphones into biosensing devices replicating the functions of expensive and inaccessible laboratory equipment. Furthermore, conditions can be semi-controlled by imposing requirements or restrictions on data acquisition, such as requiring a certain distance or viewing angle between the test/sample and the SbS [33,40,49,67,77]. In contrast, uncontrolled conditions have no specific restrictions for image capture but require additional data processing for normalization and noise removal before result interpretation [31,73]. It has been reported that for some colorimetric assays, background image correction is more efficient compared with using a light-shielding attachment to control acquisition conditions, provided that the assays are not carried out in direct sunlight [78].

Controlled conditions might result in more reliable results [54], but this is a compromise between the usability of the SbS and reducing its portability by introducing (bulky) hardware accessories. However, if the attachment improves the reliability of results from the SbS, this additional burden could be warranted [79]. Moreover, while uncontrolled conditions might improve the portability of an SbS, uncontrolled conditions impose stricter data processing requirements, unless the image correction procedures are automated. As will be discussed in detail in Part II of this review series, during the R&D and validation of SbSs, it is crucial to find an appropriate balance between the analytical performance of the SbS and its usability. Therefore, SbSs designed for use by consumers should be compact, discrete, intuitive, and if they rely on attachments, these should be interchangeable between different smartphone models.

2.3. Smartphone app interfaces for data collection

There are three main types of smartphone Apps for analytical

data collection: (i) built-in, (ii) third-party, and (iii) custom-developed Apps. These Apps can be either open-source or closed-source, with each presenting unique risks to data privacy. Proprietary or closed-source software licenses are covered by copyright, contract law, patents, and trade secrets, restricting their free use by emerging SbSs. Proprietary software is typically commercial software, including pre-installed software on smartphones. Before developers can use closed-source software, they must sign a license or enter an End User License Agreement (EULA) that defines what the user can and cannot do with the software. Closed-source software can be attractive for commercial SbSs as the ownership of the software remains the intellectual property (IP) of the company/developer. At the same time, closed-source data and handling procedures are not made public, but companies can use them for analytics. Numerous commercial companies offer Apps for transforming the user's smartphone into an optical LFIA reader based on annual subscriptions or pay-per-use licenses [14].

Data handling software is open-source when source codes are openly available. Moreover, handling is partially open-source when a portion of the software is available as open-source while the rest is proprietary (closed-source). For example, many open-source freeware Apps are still financially supported by closed-source third-party advertisements, and such embedded adware can cause in-application advertisement attacks making data vulnerable to privacy leakage [80]. Of the 886 unique articles, only 18 specifically mention implementing 'open-source' data handling. Despite this low number, open-source data handling is often considered more trustworthy, transparent, and traceable than closed-source handling. Open-source licenses are the agreements proposed by the original software developers for the other contributors to follow. Therefore, researchers and companies developing smartphone applications must understand and adhere to the most popular open-source licenses. Three frequently used open-source licenses, i.e., MIT, Apache, and GNU General Public License (GPL) [81], are summarized in plain language and ranked in order of strictness in the SI, Fig. S2.

Smartphone operating systems provide built-in camera Apps that usually have simple graphical user interfaces (GUIs) and

multiple color profiles (e.g., portrait mode, scenery, night mode, etc.) designed to be operated by non-experts for daily photography. These color profiles improve the perceptual quality of the photos; the camera App can apply color profiles before image capture or during editing. Likewise, smartphones with professional or 'pro' modes enable user control over camera functions such as shutter speed, focus, and white-balance, which can improve the sensitivity of SbSs. It was demonstrated that manually setting the SbS camera exposure time for analyzing LFAs made it possible to differentiate faint test lines (at low analyte concentrations) from the near-white strip background, thus enhancing the assay detection limit up to five-fold compared with using the automated exposure settings [82]. Yet, such camera optimization, color enhancement and proprietary closed-source modifications to image color can present challenges to scientific imaging, which requires consistent color reproduction to maintain accuracy in interpretation. Therefore, to ensure data integrity when using a smartphone camera to acquire data for analytical applications, it is necessary to disclose any color profiles or specific modes used during image capture, or any applied processing/image manipulation (such as contrast enhancement).

Numerous SbSs use third-party Apps that are freely available and (often) open-source [83]. For instance, the Android app 'Open Camera' gives users manual control over camera functionalities such as shutter speed and sensitivity towards light, enabling control over the brightness of a photo, and it even allows users to tag photos with timestamps and location coordinates. This app essentially unlocks 'pro mode' features on standard smartphone models. Another popular open-source App used by proof-of-concept SbSs includes the 'Color Picker' type Apps that enable users to specify ROIs within a photo to find their average RGB values. Compared to the built-in camera Apps, these third-party Apps allow better user control over smartphone camera, flash, and ALS sensor functions and enable manual export of the collected sensory data to universal data formats such as CSV and for local storage of the raw images (see Section 2.1.2.) on the smartphone. The advantage of such user control and data export capabilities is that it allows customized data processing and interpretation capacities, while a disadvantage is that it reduces the usability of the SbS by introducing too many manual control options. Therefore, such Apps are primarily helpful for researchers during the development stage of SbSs.

Custom-developed Apps offer the maximum degree of flexibility in the design of functionality and automation of data handling (e.g., executing a customized data handling procedure). Moreover, custom Apps enable the calling of Application Programming Interfaces (APIs) to control smartphone sensors and modules to collect, process, interpret, transfer, and store data [31]. Still, custom-developed Apps take longer to develop than existing free software and, therefore, might be unrealistic for all proof-of-concept SbSs. Software development kits (SDKs) are software tool packages that allow developers to create software or Apps for a specific platform. As such, SDKs can facilitate the development of Apps with GUIs that improve data collection and overall usability of SbSs for end-users [84]. They can be either open-source or closed-source. For instance, several 'open-source' SbS 'potentiostats' have been described in the literature (7/886) that use SDKs to create Apps that connect with the potentiostats via Bluetooth, NFC, or USB-C and use the phone as a user interface and for transmitting data to the cloud [62,85–89]. Certain commercialized smartphone-connectable potentiostats have base versions of the system that the company-delivered App controls, but SDKs are available for customizing Android applications for specific SbS purposes [90].

2.4. Data processing

Data processing procedures can be implemented online or offline to transform, normalize, and remove noise from the data collected by SbSs. See Table 2 for an overview of different approaches used in data processing for SbSs.

2.4.1. Color space transformation

The color system used in smartphone complementary metal oxide semiconductor (CMOS) sensors is the RGB system, but data processing procedures can involve transforming RGB data into different color spaces. Color spaces or models are mathematical representations, typically based on coordinates, that describe the range of colors perceivable to human vision. Color spaces reduce the inherent uncertainty related to person-to-person perceptual differences in color interpretation by using an empirical system to identify color [97]. Hardware color spaces (e.g., RGB for storage and digital display and CMYK for printing) are device-oriented, as are color spaces based on RGB (e.g., HSV/L/B). In contrast, perceptual color spaces (e.g., XYZ and LAB) more accurately describe the numerical relationship between the colors and human response to observed color change [97].

The choice of color space transformation is assay dependent, with some color spaces/channels offering more relevant information than others. For example, if an assay measures a change in color intensity, the lightness channel of LAB might be most appropriate [98], or if it measures a color change, the hue channel of the HSL could provide the most relevant information [99]. Recently, color space channel performance was compared across multiple smartphone models, and it was concluded that assays based on color change, rather than those based on changes in intensity, are the easiest to follow for the end-user [78]. While such a finding can be intuitively appreciated, the nature of the color change (different color, or different intensity) is dictated by the chemistry, not the demand, and therefore cannot always be selected. Still, the use of smart labels that can change color as a result of biorecognition events, might help to overcome such limitations [100]. Yet, so far, there has not been any attempt at standardization or harmonization of image analysis using an SbS. Moreover, the currently used approaches often lack an accurate description of the image analysis procedure, which results in a lack of literature references for implementing image analysis for emerging methods.

2.4.2. Normalization and noise removal

Normalization and noise removal minimize interference that can compromise image or video quality [93]. For example, SbSs can correct non-uniform illumination and dust on the camera lens by subtracting a background image [37], whereas morphological methods that work with the shape or morphology of features (explained in more detail in Section 2.5) can be applied to remove non-informative data [42]. Additional variation from measurement to measurement can originate from different sensors, sensor drift (i.e., small variations in sensor response), or environmental changes. Emerging SbSs require proper calibration to minimize these variations [101].

Calibration is the process of establishing the correct input-to-output mapping for the measuring system. Sensor calibration is used to measure device-dependent sensor responses, such as calibrating the SbS camera response for intensity correction [54]. Yet the inter-calibration of smartphone cameras is inherently complicated owing to the constantly evolving market [43]. Recently a standardized methodology and database (SPECTACLE) was developed for calibrating smartphone cameras (based on linearity, bias variations, ISO speed, and RGB spectral response) for radiometric

Table 2
Reported popular data processing techniques for SbSs.

Category	Name	Explanation
Color space transformation	RGB	A device-oriented color space; is widely used for color storage of images, and R, G, and B color channels quantify long, medium, and short wavelengths of light, each represented by an axis of a Cartesian coordinate system [91].
	CMY	A device-oriented color space that is mainly used for color printing. C, M, and Y are the three prime color inks, i.e., cyan, magenta, and yellow.
	XYZ	A perception-oriented color space; Defined by International Commission on Illumination (CIE) for color reproduction.
	LAB	A perception-oriented color space; Developed based on XYZ and designed to be perceptually uniform.
	HSV/L/B	A device-oriented color space. Proposed mainly to mimic the painting color mixture by artists; H, S, and V or L or B stand for hue, saturation, and value or luminance or Brightness.
Normalization and noise removal	Baseline correction	Subtracting a background signal, e.g., correcting non-uniformly distributed illumination [54] and residual current correction [92].
	Demosaicing	An algorithm for reconstructing raw images into full RGB images [50]
	Denoising and deblurring	The process of removing noise and blurring artifacts in the signal, such as spike removal by moving median filter and periodic noise removal by Fourier Transform [92], and those caused by low-quality sensors [93] and motion [91].
	White Balance	The process of correcting image color shifts due to varied colors of illumination [91].
	Sensor response calibration	Measuring and correcting non-linear sensor response to a linear input to output mapping, e.g., camera response calibration using standard calibration references [94]. Spectral and radiometric calibration of smartphone cameras [43,95]
Segmentation	Superpixel	Grouping of similar pixels to form larger homogeneous regions, known as superpixels [67]; Pixel values in a superpixel are homogenous while it is not in adjacent superpixels [96].
	ROI cropping	Cropping of the signal to only keep the region that contains information of interest [97].

and photometric measurements [43] and to promote interoperability between devices for citizen science applications.

Standard reference calibrations are those based on fixed criteria, such as color reference charts or known wavelengths of light sources. These standard references may improve the performance of SbSs but can be expensive and difficult for non-experts to access and implement [102]. Calibration can take place before, during image capture, or in post-processing. In a recent example, a method was developed for calibrating raw images alongside standard calibration targets under fixed conditions. Following raw image capture, three linear post-processing operations were applied to transform the images to a device-independent color space and extract the linearized color information for auto-detection of the target analyte [36]. Recently, the SPECTACLE database was used to calibrate wavelengths (using a reference spectrum of fluorescent light) against the RGB response from a smartphone camera for portable spectroscopy and polarimetry [43,95]. An alternative approach is to use color reference charts to normalize the colors in SbS acquired data against a set of standardized colors. In one study, images pairs were captured both with and without flash for ambient light subtraction. After decreasing the variation caused by ambient light, the images were mapped against a standard color chart allowing for conversion between different color spaces, thereby providing a device-independent mechanism for color calibration [103]. In another study, the smartphone camera's white balance was normalized to a standardized value by calibrating it against a printed grey shade reference chart [104]. In this study, it was further demonstrated that calibration can be achieved by manually imposing specific camera conditions; here, the smartphone camera's exposure was locked and SbSs images were captured in a 3D-printed lightbox that illuminated the assay with a constant smartphone-independent light source (e.g., two white LEDs) [104]. As such, calibration can help to improve an SbS by enhancing accuracy, limiting uncertainty by reducing errors in the measurements, and enabling interchangeability between devices. Still, it cannot be overlooked that such calibration would be challenging – and potentially expensive – to implement for the non-expert, so if an SbS requires calibration, this should be performed before the device is released to the end-user.

2.4.3. Segmentation

In addition to color transformation and data normalization, it is often beneficial to process data to retain informative data while

reducing the total data size. The aim of the segmentation process is to simplify or change an image into something more meaningful and easier to analyze [97,105]. As such, segmentation can be used to identify and distinguish an object from a scene background. Segmentation groups homogeneous regions and keeps any two inhomogeneous adjacent regions as ROIs [106]. In one approach, SbS-acquired images were clustered into groups of similar pixels, called superpixels [67]. After clustering, the superpixels were segmented into classes, called light background, dark background, dirt, or oocyte, making it possible to differentiate the target (oocyte) from the other parts of the image. Alternatively, data can be segmented by cropping distinct ROIs from a dataset [57]. An ROI cropping procedure was applied to data from a handheld SbS-based μ -capillary electrophoresis system for COVID-19 detection; to minimize the background noise on the fluorescent signal, the redundant video data were cropped, leaving behind only the ROI for analysis. Such segmentation approaches typically do not require a training process and are instead based on applying a pre-processing step that simplifies subsequent processing procedures. Such models have advantageous segmentation capacity, which allows the identification of ROIs from complex backgrounds. Still, these segmentation models have a higher complexity, compromising their usability on portable devices with limited computing resources. The following section provides further examples of applying learning models in SbSs.

2.5. Data interpretation and artificial intelligence

Data interpretation procedures by SbSs are required to analyze the raw or processed analytical data and provide the final test results. Data interpretation usually involves feature selection, regression, classification, and decision fusion techniques (see Table 3). Here, features are individual measurable properties specific to the processes under study.

Artificial intelligence (AI) technologies have stimulated opportunities for a wide range of smartphone analytical data interpretation and privacy protection applications. Data processing by 'AI' was used in 8 out of 886 articles. Machine learning (ML) is a sub-domain of AI that makes predictions from data, 14 out of 886 articles mention using 'machine learning' for result prediction. AI and ML can be involved in data processing and interpretation steps, such as feature selection, regression, and classification.

Table 3
Examples of data interpretation techniques for SbSs.

Category	Name	Explanation	Application/Example
Feature	Area-under-curve (AUC)	Definite integral between two points ($a + b$)	A feature used for LFIA and colorimetric assay quantification [31]
	Resonant position tracking	Position sensitive method for tracking resonant signals of SPR	SPR signal enhancement [107]
Regression	Logarithmic regression	Models situations where growth or decay first rapidly accelerates and then slows over time	Quantification of LFIAs for the detection of aflatoxin B1, zearalenone, deoxynivalenol, T-2 toxin, and fumonisin B1 in cereals [48]
	Exponential regression	Models situations in which growth/decay begins slowly and then accelerates with no bounds, or begins rapidly and slows closer to 0	Fluorescence polarization value predicted by sample viscosity [64]
	Polynomial regression	Models situations to identify a curvilinear relationship between independent and dependent variables	Predicting by the color change of pH test strip [54]
Classification	Support Vector Machine (SVM)	A supervised learning-based classifier that works by maximum marginal separating	Identification of adulterants in green tea [39]
	Random forest (RF)	A learning-based classifier that combines multiple decision trees;	Classification of superpixels for oocyte counting [67]
Decision fusion	PCA-SVM	Principal Component Analysis (PCA) for feature selection and SVM for classification	Decision fusion of smartphone image with sample spectrum for black tea evaluation [40]

2.5.1. AI for feature selection

Conventionally, deterministic and heuristic models are applied to interpret analytical data [108]. Features that require manual extraction should be intrinsic to the data, such as the area-under-curve that calculates the summed intensity of an ROI on a test strip or the signal's shape from voltammetry-based measurements [109]. When extracting features that are not intrinsic to the data set, learning-based models such as a Support Vector Machine (SVM) can automate feature selection if sufficient training data is available [110].

Currently, most ML models learn to recognize both low and high-level features, i.e., directly identifiable features in the data (e.g., object classification), and process these features from the training data without explicit coding [51,67]. Therefore, ML allows SbSs to interpret biosensor signals, even in complex sample matrices and uncontrolled scene background conditions, assuming the AI model has been adequately trained [36]. In ML approaches, selecting robust features and predicting models can improve the accuracy of data interpretation by helping the model better understand data and reducing the computation requirements enabling enhanced predictor performance [111]. For instance, researchers reported an SbS using a principal component analysis-support vector machine (PCA-SVM) model to select color, textural, and spectral features from samples to evaluate black tea quality [40]. Using this combination of features enhanced the accuracy of the SbS results from the PCA-SVM (100% for calibration set, 94.29% for prediction set) compared with the results based on individual features for color (97.14% calibration, 88.57% prediction), texture (84.29% calibration, 60% prediction), and spectra (88.57% calibration, 82.86% prediction) [40]. Furthermore, training a model to select multiple identifying features is beneficial for SbS data interpretation as it means that even if a single element is missing from a particular dataset, the algorithm would be able to work with the other features to elucidate the results.

2.5.2. AI in result interpretation (regression)

After selecting features, the AI model must correlate their related metrics to an experimental variable. A popular approach is for the algorithm to apply linear regression to interpret the result; regression calibrates a linear relationship between a selected feature (e.g., color or intensity change) and the variable to be determined (e.g., analyte concentration) [53]. When linear regression is insufficient, other nonlinear regression models, such as exponential [64], and logarithmic regression [48], can be either

manually [112] or automatically [54] applied for SbS data interpretation. The ability of a SVM to analyze multivariate, complex datasets makes them attractive and competitive models for application in SbSs. Artificial neural network (ANN) based regression models can be used to predict output variables as a function of the input variable. Still, ANNs have large sample size requirements with their performance directly related to the adequacy of their training data [113]. Therefore, regression algorithms for interpreting SbS results should be trained on large quantities of data acquired under diverse conditions (e.g., different lighting conditions, angles, times of day, recorded by different users, etc.) to ensure that the developed ANN can robustly handle variations in the data and thus be applied in the real world.

2.5.3. Conventional and federated ML

In one example, on-smartphone ML algorithms, such as a random forest (RF) and an ANN, were used to investigate how analyte concentration influenced electrochemical signal development [114]. In yet another demonstration of ML applied to an SbS platform, screening for disease in orchids was performed by training an algorithm using optical data and results from polymerase chain reaction (PCR) assays, resulting in an algorithm with 89% result prediction accuracy [115]. These studies indicate that SbSs using ANNs can largely automate data processing. However, these algorithms are based on conventional centralized ML, where data are uploaded from each connected device to a single repository, such as a cloud server, to train a generic model before distributing the model across all connected devices for interpretation. In addition, conventional ML relies on 'open data sharing' by distributing data across multiple devices and locations [56]. However, privacy concerns related to sharing sensitive or personal raw data can challenge this approach, as will be discussed in further detail in [Section 3](#).

In contrast, federated learning is an emerging AI technology that assures data privacy and enables model training on distributed devices [56]. Instead of directly transmitting user data to a central location for model training, federated learning allows users to download a model that is updated based on the locally stored user data and transmitted back for model fusion with the other updated models [56]. In this process, sensitive user data can remain secured on local devices (e.g., on the SbS) while only model updates are collected and, if necessary, transmitted. Therefore, federated learning appears promising for assuring data privacy in SbSs for PoC testing and food safety, quality, and authenticity applications

[56,116]. Furthermore, a key benefit of federated learning is that user privacy can be better maintained by only sending partial results to the cloud and not requiring storing anything directly on the device.

2.6. Online and offline data handling

After data collection, data processing can be handled online or offline. Remote data transmission to a desktop computer or a server can improve the user-friendliness of data interpretation but also creates additional risks related to stability, security, data privacy, and ownership. Herein, offline data handling is defined as the condition where data processing, interpretation, and storage can be completed without the availability of an internet connection, in contrast with online data handling, where an internet connection is obligatory.

2.6.1. Offline data handling

Offline data handling is particularly beneficial for (i) in-field/on-site measurements, (ii) for real-time detection, and (iii) when the time to result is vital. Recently, an SbS was developed that utilized an imaging App based on HSL for on-smartphone data handling, allowing for the rapid in-field detection of *Salmonella* in vegetables [99]. Such instantaneous result interpretation enables food producers to make quick, data-driven decisions about possible food safety issues. Researchers recently developed an offline, on-smartphone algorithm for monitoring living algae by real-time counting [108]. Likewise, in another example, an SbS was developed with rapid offline data handling for accelerated detection of COVID-19; the SbS used an App to record the fluorescent signal in real-time [57]. These offline approaches have the benefit of handling data directly on the smartphone and do not require an internet connection. Moreover, for offline data handling, it is acceptable to complete the data handling by either automatically or manually transmitting the data to a local server or desktop computer, where an algorithm or trained analyst can process the data before returning the processed result to the user.

2.6.2. Online data handling

In contrast, online data handling exchanges data with cloud servers providing contextual information such as color calibration models [51] and assay calibration curves [117] and enabling data persistence. Online data handling can benefit SbSs by enabling more advanced data analysis and management by accessing additional resources. One such progressive data management approach enabled by online data handling is the transfer and storage of data via blockchain. Blockchain has received increasing attention since the publication of Bitcoin [118], a popular cryptocurrency and a distributed and unchangeable ledger. Blockchain serves as an online data structure for unified and permanent data consistency among networks; it can prevent sensitive, private data from potential malicious changes or tampering while simultaneously ensuring interoperability across digital devices [118]. Blockchain technology is suitable for persisting small data and has already been successfully applied in fields such as cryptocurrency, agriculture, healthcare, and manufacturing [119–122]. However, before SbSs can benefit from handling data using blockchain, some challenges remain to be addressed, such as (i) the persistence of extensive data (e.g., multimedia – which is necessary for optical SbSs), (ii) assuring privacy of data stored in the blockchain, (iii) the development of standardized consensus mechanisms, and (iv) its energy-intensive nature (which is not environmentally sustainable) [123,124].

Despite its benefits, online data handling relies on the availability of an internet connection and can result in potential privacy

issues (discussed in Section 3). Still, numerous regions in the world lack an internet connection, including remote rural areas that could benefit from healthcare and agricultural-related SbSs. Online data transmission from these locations to cloud servers would be infeasible, whereas offline approaches can support decentralized analysis.

3. Privacy and security of data handling by smartphone-based (Bio)sensors

Using SbSs for data acquisition raises potential legal and ethical issues concerning privacy, data protection, and consumer rights. The miniaturized electronics, sensors, computing power, and connectivity that make smartphones attractive for biosensing also lead to ‘always on’ privacy risks. Personal data on smartphones can contain confidential, identifiable details of our lives, including our whereabouts, contact details, social networks, preferences, and finances [125,126]. Our personal information is vulnerable to misuse by third parties who can claim data ownership, especially when transmitted over the internet or Bluetooth, via installed Apps, or by cloud-storage providers [125]. Misuse of sensitive information endangers consumers and can lead to discrimination, identity theft, and changes in insurance policies. A deeper apprehension of the complicated legal, ethical, and practical challenges associated with using SbSs for data handling is needed to benefit from these connected technologies while minimizing potential risks for the end-user.

3.1. Privacy and personal data protection: an EU framework

Since the 1950 European Convention on Human Rights (ECHR), privacy has been a protected right of European Union (EU) citizens [127], but the ECHR was written before the digital revolution. In 1983, the first handheld mobile phone was released, ushering in a new era of technological connectivity and unprecedented privacy risks for consumers. To uphold this fundamental right in the wake of these new technologies, the European Commission (EC) published its first guidance on the processing of personal data (Directive/95/46/EC) [128] and privacy by the telecommunications industry (Directive/97/66/EC) [129], defining *personal data* as “any information that can directly or indirectly identify a data subject” and *processing* as “any operation including recording, collecting, organizing, storing, using, transmitting, or destroying of that data”. Regulation (EC) No 45/2001 closely followed in 2001, giving individuals legal rights related to the movement and processing of their data by EU institutions [130]. Soon after, the first smartphone was commercialized, quickly followed by camera phones with wireless internet connectivity [3]. In 2002, the ‘e-privacy directive’ was implemented (Directive 2002/58/EC) [131], outlining novel risks related to these new technologies and preparing the EU for the upcoming digital age. These regulations were enshrined into EU law in 2009 under the Charter of Fundamental Rights of the EU (CFR) [132]. Furthermore, the CHR reaffirmed the ‘right to privacy’ and ratified the ‘protection of personal data’, providing data subjects with specific legal rights regarding their data [133].

In 2018, the EU implemented the world’s firmest data protection legislation, the General Data Protection Regulation (GDPR), a globally influential law unifying EU directives and regulations related to personal data handling. The GDPR’s jurisdiction extends to all smartphone Apps that collect and process data of EU citizens regardless of where the App is operated or what it is used for [134]. Moreover, the GDPRs underlying principles: consent, privacy, security, and fair data collection, provide firm guidance on how to handle smartphone-acquired personal data correctly. Many countries have similar data protection reforms, including Australia,

Brazil, Switzerland, China, Canada, and a multitude of state, federal, and local frameworks in the United States of America (USA), such as the 1996 Health Insurance Portability and Accountability Act (HIPAA 1996) [135]. For example, HIPAA safeguards 'electronically protected health information' to ensure confidentiality, integrity, and availability of healthcare information. Still, HIPAA's privacy rule permits the disclosure of personal information to covered entities, including healthcare providers, insurance companies, and business associates, presenting unique ethical considerations for emerging SbSs in the USA [136]. While the following sections are focused on privacy related to SbSs, these issues exist for all devices that generate, process, and transmit data digitally.

3.2. Data handling for smartphone-based (bio)sensors

When acquiring, processing, transferring, and storing data with any digital device, including SbSs, there are many important privacy-related considerations to reflect on, as summarized in Table 4. These considerations include assessing at which stage(s) consent should be obtained, how privacy will be protected, who will be responsible for data security, where data will be stored or to whom it will be transferred, and when metadata collection is appropriate.

3.2.1. Consent

A major ethical challenge is making people aware of the complicated privacy risks that emerging SbSs present so that users can make informed decisions on whether to consent to use such devices. Demonstrating consent is a crucial requirement for processing personal data under the GDPR. In practice, consent requires being transparent with users about how their data will be collected, used, stored, and whether it will be shared with other parties [175]. Article 7 of the GDPR states that consent must be given freely. However, individuals can choose to place conditions or limits on their consent. Apps must obtain user consent to access various smartphone features through granted permissions. On Android devices, permissions are classified as 'dangerous' if they threaten privacy, particularly Apps that request access to body sensors, cameras, calendars, contacts, geolocation, microphone, calling, texting, and storage. Unsurprisingly, SbSs (especially optical SbSs) typically require access permissions to at least one of these on-device features.

According to the GDPR, consent requests for processing personal data should be distinct from other agreement policies and based on positive 'opt-ins' such as digital signatures or fingerprint scans rather than default procedures (e.g., pre-ticked boxes). Moreover, consent must be obtained for each type of processing, allowing

users to 'opt-out' of processes or withdraw their data entirely if they desire (i.e., partial consent) [137]. Currently, most consent-based control access models are binary, and do not provide the user with a third option of partially providing consent. Implementing models for partial consent could uphold the GDPR by improving user understanding of what processing they are consenting to and by ensuring that permissions are not granted by default. Currently, many websites and Apps comply with the GDPR by requesting consent for data processing via cookie banners with granular opt-in/out options. However, one could argue that the ubiquity of such cookie banners on every digital interface might lead to consumers automatically accepting permissions without thoroughly reading what they are consenting to. Therefore, for SbSs handling sensitive healthcare data, consent should be explicitly re-obtained before each stage of data collection, processing, storage, and sharing of the data rather than using cookies as uniform (and quickly forgotten) consent management upon installation of the software.

Despite being a cornerstone of ethical data handling, only 7 out of 886 articles mentioned obtaining user 'consent' before SbS-based data collection/handling in their abstracts/keywords. For example, in a survey focusing on the end-user perspectives of an electrochemical SbS for monitoring glucose and lactate levels, 86.1% of the 383 participants agreed that explicit consent must be obtained before their data can be accessed [137]. Surveys such as this are important as they reveal how much (or little) end-users understand about data security and consent. Interestingly, a study evaluating the usability of smartphone interfaces for diabetes monitoring reported gaining consent from participants before conducting the assessment questionnaire but did not mention how or at which stage consent was obtained before using the SbS for processing the data [141]. Another study reported receiving 'informed written consent' from 10 study participants (age: 18+) before using an SbS as an optical pulse oximeter for measuring the oxygen saturation of a user's blood [140]. In this study, a trained technician in a centralized laboratory performed the measurements on a stand-alone smartphone; the App, which meets Food & Drug Administration (FDA) and international standardization organization (ISO) requirements, collected confidential medical data but otherwise did not infringe on individual participant's privacy. Likewise, a study using the SmartPhone Oxygenation Tool (SPOT) for remote patient wound monitoring reported obtaining written consent from all study participants. Still, this SbS was also used in a controlled, clinical PoC setting, minimizing the personal privacy risk for the participant [5].

Interestingly, these approaches did not incorporate smartphone Apps to acquire digital consent, still opting for written permission,

Table 4
Ethical data handling principles from GDPR.

Name	Basic principles	GDPR	SbS ref
Consent (section 3.2.1.)	Consent must be demonstrable; consent in an intelligible and easily accessible form, using clear language; data subject can withdraw consent at any time; consent must be given freely	Article 7: Conditions for consent	[5,137–141]
Privacy (section 3.3.)	Data protection through technology design; data minimization, storage limitation, purpose limitation	Article 25: Privacy by Design	[137,142–151]
Data security (section 3.4.)	Ensure appropriate security measures to protect personal data; pseudonymization & encryption of personal data; confidentiality, integrity, availability & resilience of processing systems; restoring access to data when access has expired	Principle (f): Integrity and confidentiality (security); Article 32: Security of processing	[152–156]
Data transfer & storage (section 3.5. & 3.6.)	Data must not be kept longer than needed; policy stating retention periods; data periodically reviewed; data can only be kept longer for archiving, scientific or historical research; strict restrictions for processing personal data outside of the EU	Principle (e): storage limitation; Article 44: General principle for transfers	[150,157–165]
Fair (meta)data collection (Principle A) (section 3.7.)	Must identify valid grounds (lawful basis) for collecting and using personal data; must not breach data laws; data processing must be fair; must be transparent and honest about how data will be processed	Principle (a): lawfulness, fairness, and transparency	[153,166–174]

possibly because these studies were carried out using SbSs in centralized facilities with pre-existing procedures for obtaining clinical consent. A study reporting on an SbS for influenza self-testing obtained user consent via the App before providing users instructions on administering the test and recording and transmitting the result [138]. Obtaining digital consent is preferable for SbS-guided self-testing, whereas traditional consent procedures may be more appropriate for clinical testing. Despite the above examples focusing on consent, none addressed the potential privacy risks that might arise from using smartphones as data collection devices.

3.3. Privacy

'Privacy by design' is a key requirement of the GDPR (Article 25) that puts the responsibility of digital privacy protection on the data processor. Privacy safeguards include data minimization, storage limitation, and purpose limitation, meaning that only necessary data can be collected and stored for the shortest time with access limited only to authorized parties. Still, such privacy-preserving approaches complicate matters for SbS-based data collection, where long-term storage or the accumulation of long-term data might be necessary to build up complex pictures. Likewise, these privacy strategies could be problematic for AI approaches that adhere to open data principles, as mentioned in [Section 2.5.3](#). However, as stated in principle (e) of the GDPR (see [Table 4](#)), longer-term retention of personal data is acceptable for scientific, historical, or statistical research purposes so long as it is first adequately anonymized.

3.3.1. Anonymization

Preservation of personal or commercial privacy is crucial, yet it is only mentioned in 13 of the 886 articles when searching 'privacy' in their abstracts/keywords, indicating it is a neglected issue for emerging SbSs. Of these 13 papers, 5 use data 'anonymization' as a privacy-preserving technique. Data anonymization facilitates the processing of personal data so that it cannot be attributed to a specific data subject without the use of additional information. Examples include *k*-anonymization and clustering techniques which remove personal identifiers from data and partition anonymized data with similar attributes into categorical subsets, thereby obscuring any identifying information about an individual and protecting personal privacy [149]. Data anonymization protects information by encrypting or erasing identifying features (identifiers) that connect stored data to individuals/test results. Commonly applied data anonymization techniques include replacing private identifiers with pseudonyms (data pseudonymization) [149], swapping attributes that contain identifiers (swapping) [176], and hiding data with altered values (data masking) [177]. Safeguards vary from basic such as swapping patient samples with study IDs, to more advanced strategies [176]. Advanced techniques can include tokenization and encryption, which transform personal data into unreadable data that can only be re-accessed using a unique token or key, allowing access to user-generated data while maintaining privacy protection [139]. Yet, data anonymization by itself may not provide adequate privacy protection for SbSs handling sensitive healthcare-related data. Privacy can be better protected by applying pseudonymization at multiple points in the data processing cycle.

Another important consideration is the use of publicly available information for data re-identification or de-anonymization [178]. Anonymized data prevents the data subjects from understanding how their participation contributed to a scientific study, which in turn could limit public trust in research and decrease the number of willing participants. There is clearly a fine line between

safeguarding privacy through anonymizing data and satisfying participant curiosity by providing individual research results.

3.3.2. Encryption

As shown above, encryption can help to preserve personal privacy. Still, hackers can access even encrypted data by retracing the anonymization process, leaving potential users of SbSs susceptible to privacy violations. Moreover, not all smartphones have encryption built-in as a default; over 10% of Android devices are still operating on Android version 6.0, which does not support data encryption [179]. Ultimately, this leads to a digital security divide, where older smartphones running on outdated operating systems no longer receive security updates putting them at a greater privacy risk. An alternative security approach, sign-cryption, can guarantee confidentiality and data integrity by combining a digital signature and encryption in a single step. Recently, researchers proposed the certificate-less aggregate sign-cryption scheme (CLASC) as a robust security framework for SbSs [177]. The CLASC approach provides confidentiality, integrity, mutual authentication, and anonymity, upholding personal privacy to a higher standard than anonymization alone. In another example, a CLASC was developed to secure sensitive location data from smartphone crowd-sensing participants, protecting them against data privacy attacks [180]. A combination of pseudonymization and anonymization techniques can provide additional protection, where data is first made anonymous by removing any personal identifiers and then encrypted before storage [108]. When data is anonymized adequately with all identifiers removed, it no longer falls under the scope of the GDPR, leaving companies free to collect such data without consent and store it indefinitely.

In addition to personal privacy, company/commercial data contains sensitive information vulnerable to data theft. To protect confidential company information from digital attacks, data on employee smartphones/tablets should always be encrypted and only transferred through encrypted channels [181]. The industry encryption standards are S/MIME (digital correspondence) and AES-256 (data encryption). S/MIME is the predominant method for encrypting sensitive emails; it uses separate keys for encryption/decryption (private) and digital signature (public) [150]. AES-256 uses the same 256-bit key to encrypt and decrypt data. In addition to these standards, companies often require end-to-end encryption for digital correspondence, restricting access except for the sender and recipient. The situation is more complex for dynamic group-based (2+ participants) applications that communicate via secure channels to avoid disclosing confidential and private information to unauthorized users. Group-based applications require lightweight key management frameworks capable of switching, deleting, and, if necessary, reissuing access keys based on group membership status [182].

3.4. Data security and authentication

Data security means safeguarding digital information from unauthorized access, corruption, loss, or theft. Security is an essential component of the GDPR; the regulation mandates that any researcher or company wishing to process personal data, track people's locations, monitor publicly accessible spaces [183], or use new technologies (such as smartphones) to process data, are required first to submit a Data Protection Impact Assessment (DPIA), or in the context of scientific research a Data Management Plan (DMP) [154]. These assessments should demonstrate how and why data will be processed and transparently outline the potential risks and appropriate security mechanisms to protect against them.

Authentication is one of the core principles of data security that keeps unauthorized users from accessing sensitive information.

However, few articles about SbSs, report any ‘security’ measures (18/886), let alone authentication measures. User authentication mechanisms are broadly classified into three groups based on: (i) something the user knows (knowledge-based), (ii) something the user has (token-based), or (iii) something the user is (biometric-based) [184].

3.4.1. Knowledge-based authentication

Knowledge-based authentication is the weakest form, requiring only some ‘secret’ information such as a password (text, graphical or pattern-based) or Personal Identification Number (PIN) to unlock the device. When knowledge-based approaches are applied, password management systems that prevent the password from being entered in readable text format can improve security by keeping the password secure even if the password manager is compromised [185].

3.4.2. Token-based authentication

Conversely, token-based authentication relates to the tokenization and anonymization privacy-preserving techniques discussed in Section 3.3. Approaches can include QR codes and two-step authentication (first requiring a password and then using a one-time passcode) or can use keys generated by an external device or service provider to access the data. The authentication mechanism can even be part of the data acquisition process, as demonstrated for an SbS Biomedical microelectrochemical system (BioMES)-based sensor for portable biomarker detection [153]. Here, the BioMES stored the encryption key that remained with the user, and only authorized people could decrypt it using the smartphone App. Still, storing the key on a physical system (e.g., the BioMES-sensor) has some disadvantages, including potential damage, loss, or theft of the platform. A similar method was used for sensor-based analog signal encryption, where a smartphone transmitted results to the cloud for analysis before being sent back to the user for decryption with the key stored on their smartphone [151]. Both approaches obfuscated the analog signals (impedance measurements) before transferring the data and only authorized access to users with authentication keys, providing a robust safeguard. Comparably, a privacy-preserving body sensor data collection and query scheme (SPQC) was reported for transforming body sensor data into multidimensional data before converting each dimension into ciphertext and uploading it to the cloud via a smartphone. The SPQC further secures confidential data by restricting access to only authorized users through cloud query services [155]. As introduced in Section 2.6.2., blockchain can promote enhanced data security by making data traceable. A recent study reported a token-based authentication approach that uses attribute-based encryption (ABE) to protect confidential health data transferred via blockchain [186]. In this study a smart contract was deployed on blockchain to control data access; encrypted data was only accessible following authentication via the data access App installed on authorized devices. This example demonstrates the future potential of blockchain for data security of emerging SbS, so long as the previously discussed limitations are overcome.

3.4.3. Biometric-based authentication

The third group of authentication mechanisms, biometric-based authentication, involves using a person’s physiological or behavioral attributes for authentication. Smartphones can authenticate a user based on physiological features collected by connected body area networks (BANs) [156]. For example, biometric-based authentication can lock/unlock SbSs using fingerprint, facial or voice recognition. Moreover, biometric-based authentication can combine with wireless body area networks (WBANs), sensors that attach to a person’s clothes or body to collect data that is

transferred to an SbS within a limited range. WBANs can even collect data from electrocardiogram (ECG) sensors and use representative physiological features gathered from an individual’s ECG records as specific biometric parameters during authentication [187].

Moreover, additional privacy-preserving tools such as pseudonymization and aggregation can strengthen biometric-based authentication [188]. As always, authentication measures should be fit-for-purpose for the intended SbS application. For example, if an SbS is being used for analysis that requires the user to wear protective gloves, a biometric-based authentication using fingerprint ID would not be appropriate and facial recognition might be preferred. At the same time, biometric-based authentication assumes the stability of the human body, when, in reality, bodily features change substantially over time: faces age, fingerprints become worn, and appearances can alter by injury (e.g., scarring), disease, (cosmetic) surgery, and changes in weight [189]. As such, any methods using biometrics should regularly reobtain biometric measurements to ensure that authentication is not compromised.

3.5. Data transfer

A key advantage of SbSs is the possibility to wirelessly transmit data via cellular data, Wi-Fi, Bluetooth, or, Near Field Communication (NFC); for a detailed technical description of wireless SbSs readers should refer to Ref. [190]. However, there are risks associated with wireless data transfer; if a network is not secure, people with wireless-enabled devices within the vicinity can ‘piggyback’ onto the connection and possibly intercept the data [191].

3.5.1. Online wireless data transfer

Data transfer to cloud servers via cellular data or ‘Wi-Fi’ is convenient (26/886 publications) but requires a stable internet connection for online processing (as discussed in Section 2.6.2). The HyperText Transfer Protocol Secure (HTTPS) enables secure communication over computer networks securing user data through encryption. The protocol is a default in iOS (2016) and Android (2018) native Apps, allowing secure data transfer from connected smartphones to cloud drive servers [80]. However, when transferring data online, third-party networks often record meta-data or sell data for consumer analytics purposes [80]. Data sharing is technically permissible, usually covered by fine-print privacy policies and service agreements, but it violates user expectations of fair data collection [192]. Data transmitted to cloud servers from SbSs can be embedded with watermarks to improve security and authentication [159,168] or use an aggregate sign-cryption-based scheme to secure data in transit [158,159].

3.5.2. Offline wireless data transfer

Many SbSs do not need to be online for data transfer; ‘Bluetooth’ (32/886) and ‘near field communication (NFC)’ (10/886) technologies do not require internet connections for data transfer. Still, both approaches only have a limited range (Bluetooth = 10–15 m, NFC = 0.1 m) requiring proximity [193,194]. Unlike battery-draining Bluetooth-based devices, NFC-based sensors are battery-free and affordable. Moreover, NFC sensors can offer protection against piggybacking or data sniffing, as recently demonstrated by a study using NFC-embedded clothing for continuous monitoring of spinal posture, temperature, and gait during exercise [195]. Another study used a battery-free, card-sized NFC tag integrated with an electrochemical SbS for diagnosing hepatitis B. The measurement data was transmitted to a smartphone App in real-time before being transferred to a computer for subsequent offline analysis [162]. As discussed in Section 2.6.1., there are several advantages for SbSs operating without an internet connection, and

those SbSs that use Bluetooth or NFC for data transfer are well suited for offline approaches.

3.6. Data storage

Typically, built-in smartphone cameras directly store images or videos in the on-device image gallery provided by the operating system. Most third-party and custom-developed camera Apps also record the collected data in the image gallery. Data stored in this approach includes independent multimedia files with embedded metadata such as image dimensions, resolution, and camera parameters that other Apps can access if the smartphone user grants permissions. In addition, self-contained software libraries, such as Android's SQLite, can store data and provide database management [196]. However, such data storage is usually without backup and is prone to tampering or malicious changes [197]. In comparison, system administrators manage data stored in the cloud. Advantages of this approach include extendable computing resources and availability of contextual information. Still, such storage leaves data vulnerable to privacy attacks.

3.6.1. Data storage for corporations

Institutions and corporations transferring or storing sensitive or private information on smartphones are vulnerable to corporate espionage and should uphold data security through various access controls such as the knowledge, token, and biometric-based approaches discussed in [Section 3.4](#). Companies operating bring-your-own-device policies require employees to only store confidential company data in a secure compartment of their smartphone to which the company IT department has unrestricted access [198,199]. Still, on-device storage leaves data vulnerable to hacking, theft, or physical damage [181]. Companies can opt to use external smartcards/microSD cards, which are returned to the company with digital certificates to protect confidential information and prevent on-device retention of data [80]. However, these cards are also at risk of being lost.

Instead of storing data on employee smartphones, companies handling confidential data can use SbSs to unidirectionally transfer data to secure servers. Unidirectional data transfer can be necessary to provide additional security and prevent smartphone Apps from accessing confidential data. For example, recently, an augmented reality smartphone App was developed that transferred data asynchronously to secure servers through specialized network interfaces [163]. This asynchronous transfer limited the on-device data storage to protect the user's location during combat operations. Another study implemented off-device data storage with App-based data acquisition and synchronization with a secure cloud server to rapidly detect Azole-resistant moulds in clinical and environmental samples [164]. Comparably, a medical SbS for monitoring chronic bronchitis used a smartphone App for classifying clinical data and transmitting the anonymized data to secure cloud servers for further encryption and processing [200].

While undoubtedly making data transfer and storage more secure, these additional authentications are burdensome from an end-user perspective. In establishing policies concerning different security levels, and the associated operational burden on the user, there is a balance between the two. Depending on the target users and whether they are private citizens or companies, data security and usability without too many constraints will play essential roles in technology acceptance by those various user groups.

3.7. Big data: fair (meta)data collection

Smartphones are constantly collecting data from us; the accumulation of this information from billions of people worldwide is

big data. Big data relates to the volume, variety, and velocity of data; mass analysis of this data generates enhanced insights into specific patterns or trends for decision-making and process automation [201]. In recent years, the massive increase of data from connected devices has accelerated the rise of a 'data-driven' era where metadate analytics facilitate data-driven decision-making across multiple fields, including health [166], food safety [167], environmental safety [168], and forensics [169].

However, the fundamental right to personal data protection fully applies in a big data context, with a vital cornerstone of the GDPR being the lawfulness, fairness, and transparency principle [170]. The principle specifies that there must be a valid reason for collecting and processing personal data to prevent unlawful actions from being applied to said data. Moreover, the regulation imposes stricter conditions for processing special categories related to health, race, politics, sex life, sexual orientation, genetics, or biometric data. Notably, fair data collection means that data can only be collected and processed as expected and protects data from misuse in any misleading or detrimental way. Therefore, it is vital to have clear and honest communication about the intended use of data so as not to coerce individuals into sharing unwanted information [202]. Still, the situation becomes concerning when commercial devices connected via smartphone Apps gather private information, including location, user names, phone numbers, and financial information, that is shared with third parties [172]. Therefore, SbSs that handle sensitive health-related data must be transparent regarding how they will exploit any metadata.

Nevertheless, mining metadata could result in ethical issues surrounding consent, for example, if a user consents to data collection for one purpose but does not consent to reusing their data for analytics purposes [173,202]. However, consent becomes less clear for big data; it can be difficult to 'opt out' from a data analytics set, especially when 'opting out' of a dataset could identify a company or individual. Despite this, metadata can be used for big data purposes so long as appropriate safeguards ensure compliance with the GDPR [170]. The guiding principles of FAIR (Findability, Accessibility, Interoperability, and Reuse) [203] provide a solid basis for ethical metadata collection that could be useful for emerging SbSs [204]. Moreover, the FAIR guidelines adhere to the principles of Good Research Practice (GRP), as will be further discussed in Part II of this review series. Finally, the security of big data is vital for personal and organizational privacy, as individuals and companies can be at risk from cyber criminals due to the information they store. While tedious, proper data governance improves its usefulness, accessibility, and security. Still, one could argue that bureaucracies such as the GDPR are suppressing the field of big data. On the other hand, without effective governance, SbS-acquired big data can be and has been used for intensifying mass surveillance of individuals and organizations, as discussed further in the **Case Study**.

4. Case study: near real-time dynamic data handling for mapping of infectious disease

Connected SbSs can improve accessibility to healthcare through (i) guided self-testing and (ii) (near) real-time data transfer for reporting results and mapping disease outbreaks. Moreover, SbSs can facilitate surveillance of rapidly spreading infectious diseases creating geospatial maps of emerging outbreaks by geotagging positive self-test results from SbSs [9,205–207]. Studies have demonstrated that smartphone-guided self-testing for HIV is safe, accurate, and acceptable [208,209] and can be combined with digital partner notifications (a.k.a., contact tracing) while still maintaining complete security, privacy, confidentiality, and data anonymity [157,209].

Self-testing and disease surveillance are necessary for monitoring the spread of public health issues, as exemplified by the COVID-19 pandemic. The pandemic has stimulated scientific and technological innovation, emphasizing the need for accurate, consumer-operable self-tests integrated with smartphone detection for data handling and result interpretation [210–215]. In one COVID-19 SbS, the App controls the smartphone camera and flash to capture images under fixed illumination and uses an in-App artificial neural network (ANN) for result interpretation, guaranteeing complete privacy of results [214]. In a commercial, FDA-approved COVID-19 SbS, the analyzer can be connected offline via Bluetooth to integrate with an App on the user's smartphone. In addition, the App automatically reports encrypted, anonymized data to health authorities when connected to WiFi through a secure HIPAA-compliant cloud connection [216].

At the same time, the pandemic has accelerated the uptake of digital surveillance technologies in the form of physical contact tracing Apps which might pose a risk to privacy. Properly aggregated (pseudo)anonymized smartphone data can enable mobility and population estimates to assist epidemiologists and policymakers in better understanding the spread of infection [125,217]. Apps can collect proximity data about infected individuals and their wider social networks using precise geo-location data or the cellular module, Wi-Fi, or Bluetooth to communicate with phones in the vicinity without tracking the user's location [218,219]. This information can help limit disease propagation and save lives, but such surveillance also poses unique privacy risks. Justifiable concerns over data security and loss of personal privacy have resulted in low tracing App installation rates, undermining these tools' efficacy [217]. Privacy policies should transparently outline how data will be collected and used to promote uptake of these Apps [200]. Transparency is jeopardized when end-users cannot comprehend what they are consenting to. A recent assessment of seven COVID-19 contact tracing Apps revealed that their privacy policies had readability levels that were considerably more advanced than what the average individual could understand [220]. Critically, this leads to unethical and unfair data handling practices because the user cannot give *informed consent* for something they do not understand. It could be argued that informed consent does not apply when a lack of individual consent has the potential to negatively affect society (as with the spread of COVID-19). While it is true that countries that implemented quasi-mandatory digital contact tracing have higher rates of app installation [221], it cannot be overlooked that enforcing the use of such apps hinders users' capacity to freely provide consent [222].

A key concern for many is that the digital surveillance tools being legalized for the current emergency, without adequate checks and balances, might still be used after the pandemic [126]. Therefore, to minimize privacy impact and ensure fair data collection, it is crucial to be transparent regarding the proposed and actual data use, including future privacy [219,223]. In the end, there are crucial trade-offs to consider between society-based digital contact tracing and privacy protection [224,225].

Currently, these smartphone-based strategies run in parallel. Still, it seems likely that we will soon see an integrated approach that guides self-testing, records results, and interprets data within an App linked with privacy-preserving contact tracing. The combination of these approaches, smartphone-based biosensing with GDPR-compliant digital contact tracing, would be a powerful tool in the fight against infectious diseases and numerous other applications.

5. Perspectives & proposed best practices for the development of emerging smartphone based (bio)sensors

The field of (bio)sensing is increasingly digitalized, miniaturized, and interconnected. In this past decade, smartphone-based biosensing has emerged as an important trend for decentralizing and democratizing science by increasing access to testing, interpretation of results, and data storage for various uses. There are already myriad proof-of-concept optical and electrochemical SbSs for clinical, food safety, environmental monitoring, and forensics. At a minimum, these SbSs utilize some built-in smartphone function to acquire, store, or transfer data; for optical SbSs, the most used feature is the camera and flash, whereas for electrochemical SbSs plug-in potentiostats that directly draw power from the smartphone are most often used. During the R&D stage of any SbS, developers should consider how the SbS will be used. For example, if the SbS is intended for proof-of-concept or research-use-only purposes, it could be appropriate to use the smartphone solely to collect and transfer raw data to a computer for further processing and (image) analysis.

Similarly, SbSs in the proof-of-concept stage could benefit from using already available free and open-source software for data handling, which could save time and resources compared to designing a custom App for each (academic) purpose. On the other hand, commercial companies marketing SbSs should develop dedicated Apps capable of safely handling private data that use appropriate GUIs to facilitate secure data collection and ease the user experience. Commercial SbSs might still rely on online data handling by transferring collected data to cloud servers for analysis and interpretation before returning the result to the end-user. However, this online handling should require minimal user involvement and impose the least privacy risk. Otherwise, commercial SbSs might incorporate algorithms so that data can be handled on the smartphone while offline, anytime, anywhere by an authenticated user. As discussed, perhaps conventional ML approaches are not the most appropriate for implementation in SbSs when considering ML's core principles of open data sharing. Instead, software developers for emerging SbSs could consider using federated learning approaches that better uphold data security by training algorithms across multiple decentralized devices while keeping raw data acquired on the user's SbS.

Another option for emerging SbSs in a PoC setting could be to develop SbSs based on standalone smartphones with offline data processing that is dedicated to the task. Not only would standalone SbSs promote robust privacy-preserving techniques, but they would also be easier to validate from an R&D perspective. Considering how regularly consumers upgrade their smartphones, it would be sensible for emerging SbSs to be tested on different smartphone models, and where possible calibrated in a device-independent fashion to minimize inter-phone variation. Yet, the multitude of existing smartphone models makes it unrealistic to tailor calibration to each individual consumer smartphone, making the use of a standalone SbS attractive. On the other hand, standalone SbSs would be of limited use to consumers who likely already own a smartphone device and who might not want a different device just for biosensing applications.

The most desirable approach for consumer-focused SbSs is to transform a user's smartphone into a biosensing device by installing secure Apps and if necessary, attachable or plug-in auxiliary equipment. Of course, the installation of Apps on the same smartphones that consumers use for daily communication,

photography, finances, and other essential tasks, requires strict privacy-preserving techniques, as outlined in the GDPR. As has been discussed, the core principles of the GDPR related to consent, privacy, security, transfer, storage, and fair data collection are fundamental for any smartphone Apps that collect and process data from EU citizens. These principles can and should guide best practices when developing Apps for emerging SbSs.

Still, while additional authentication measures required by the GDPR principles increase the security of SbS-based data collection, transport, and storage, they are also cumbersome for the end-user. Therefore, developers of emerging SbSs must find a middle ground concerning the authentications required based on different security levels and the associated operational burden these measures pass on to the end-user. To find a balance, SbSs must be fully transparent in their intended uses of collected data, and should regularly re-acquire consent from end-users to guarantee that they (still) grant permission for said data handling. Of course, data security and upholding the GDPR are of critical importance, but it is also vital that end-users adopt and accept SbSs, which they may be less inclined to do with too many (or too few) data security restrictions.

Part II of this review series will unravel the best practices for emerging SbSs from an R&D and end-user perspective, focusing on the sustainable design, development, and validation of these bio-sensing devices. Likewise, Part II will consider the wider impact of such SbSs on consumers allowing for a holistic reflection on their implementation and acceptance in society.

Author contributions

Ross, G.M.S., Zhao, Y., Salentijn, G.IJ. *Conceptualization*; Elliott, C.T., Nielen, M.W.F. Salentijn, G. IJ. *Funding acquisition*; Elliott, C.T., Nielen, M.W.F., Rafferty, K. Salentijn, G.IJ. *Project administration*; Elliott, C.T., Nielen, M.W.F., Rafferty, K. Salentijn, G.IJ. *Supervision*; Ross, G.M.S., Zhao, Y. *Visualization*; Ross, G.M.S., Zhao, Y. Salentijn, G.IJ. *Roles/Writing - original draft*; Ross, G.M.S., Zhao, Y. Bosman, A.J., Geballa-Koukoulou, A., Zhou, H. Elliott, C.T. Nielen, M.W.F. Rafferty, K. Salentijn, G.IJ. *Writing - review & editing*.

Funding statements

This project has received funding from:

The European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 770325 (FoodSmartphone).

The European Union's Horizon 2020 research and innovation program under grant agreement No. 101016444 and is part of the PHOTONICS PUBLIC PRIVATE PARTNERSHIP (PhotonFood).

Funding and support from the Key Laboratory of Intelligent Preventive Medicine of Zhejiang Province (2020E10004).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

ABBREVIATIONS

ALS	Ambient light sensor
API	Application programming interface
App	Application

AI	Artificial Intelligence
ANN	Artificial neural network
ABE	Attribute-based encryption
BioMES	Biomedical microelectrochemical system
CLASC	Certificate-less aggregate sign-cryption scheme
CFR	Charter of Fundamental Rights of the EU
CFA	Color filter array
CMOS	Complementary Metal-Oxide-Semiconductor Transistor
CNN	Convolutional neural network
CMY	Cyan, magenta, yellow
CPU	Center Processing Unit
CSV	Comma Separated Value
DPIA	Data protection impact assessment
EULA	End User License Agreement
EC	European Commission
ECHR	European Convention on Human Rights
EU	European Union
FNN	Feedforward neural network
FAIR	Findability, Accessibility, Interoperability and Reuse
FDA	Food & Drug Administration
FPS	Frames per second
GDPR	General Data Protection Regulation
GPL	General public license
GPS	Global positioning system
GHz	Giga hertz
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act (HIPAA 1996)
HSV/L/B	Hue, saturation, value/lightness/brightness
HTTPS	Hypertext Transfer Protocol Secure
IoT	Internet of Things
LFIA	Lateral Flow Immuno Assay
LOD	Limit of Detection
LAB	Luminosity, xA, aB
Mbps	Megabits per second
ML	Machine Learning
NFC	Near field communication
PIN	Personal identification number
PA	Physical activity
PoC	Point of care
PoN	Point of Need
PCR	Polymerase chain reaction
PCA	Principal component analysis
QR	Quick response
RF	Random forest
RGB	Red, green, blue
ROI	Region of Interest
R&D	Research & Development
SbS	Smartphone based sensors
SPOT	SmartPhone Oxygenation Tool
SDK	Software Development Kit
SD	Storage Device
SVM	Support vector machine
SPR	Surface plasmon resonance
ISO	The international organization for standardization
WBAN	Wireless body area network
SSL	Secure sockets layers
TLS	Transport layer security

Appendix A. Supplementary data

Supplementary data to this article can be found online at <https://doi.org/10.1016/j.trac.2022.116863>.

References

- [1] M. Barton, R. Budjac, P. Tanuska, G. Gaspar, P. Schreiber, Identification overview of industry 4.0 essential attributes and resource-limited embedded artificial-intelligence-of-things devices for small and medium-sized enterprises, *Appl. Sci.* 12 (2022) 5672. <https://doi.org/10.3390/app12115672>.
- [2] <https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/>, ((n.d.)).
- [3] I. Hussain, A.K. Bowden, Smartphone-based optical spectroscopic platforms for biomedical applications: a review, *Biomed. Opt. Express* 12 (2021). <https://doi.org/10.1364/BOE.416753>.
- [4] A. Trifan, M. Oliveira, J.L. Oliveira, Passive sensing of health outcomes through smartphones: systematic review of current solutions and possible limitations, *JMIR Mhealth Uhealth* 7 (2019). <https://doi.org/10.2196/12649>.
- [5] K. Kaile, C. Fernandez, A. Godavarty, Development of a smartphone-based optical device to measure hemoglobin concentration changes for remote monitoring of wounds, *Biosensors* 11 (2021). <https://doi.org/10.3390/bios11060165>.
- [6] S. Dutta, Point of care sensing and biosensing using ambient light sensor of smartphone: critical review, *TrAC, Trends Anal. Chem.* 110 (2019). <https://doi.org/10.1016/j.trac.2018.11.014>.
- [7] H. Nam, K.-H. Seol, J. Lee, H. Cho, S.W. Jung, Review of capacitive touchscreen technologies: overview, research trends, and machine learning approaches, *Sensors* 21 (2021). <https://doi.org/10.3390/s21144776>.
- [8] Y. Zhao, F. Bacao, How does the pandemic facilitate mobile payment? An investigation on users' perspective under the COVID-19 pandemic, *Int. J. Environ. Res. Publ. Health* 18 (2021) 1016. <https://doi.org/10.3390/ijerph18031016>.
- [9] C.S. Wood, M.R. Thomas, J. Budd, et al., Taking connected mobile-health diagnostics of infectious diseases to the field, *Nature* 566 (2019) 467–474. <https://doi.org/10.1038/s41586-019-0956-2>.
- [10] A. Domin, D. Spruijt-Metz, D. Theisen, Y. Ouzzahra, C. Vögele, Smartphone-based interventions for physical activity promotion: scoping review of the evidence over the last 10 years, *JMIR Mhealth Uhealth* 9 (2021), e24308. <https://doi.org/10.2196/24308>.
- [11] K.-J. Brickwood, G. Watson, J. O'Brien, A.D. Williams, Consumer-based wearable activity trackers increase physical activity participation: systematic review and meta-analysis, *JMIR Mhealth Uhealth* 7 (2019), e11819. <https://doi.org/10.2196/11819>.
- [12] T. Alawsi, Z. Al-Bawi, A review of smartphone point-of-care adapter design, *Engineering Reports* 1 (2019). <https://doi.org/10.1002/eng.2.12039>.
- [13] H.N. Chan, M.J.A. Tan, H. Wu, Point-of-care testing: applications of 3D printing, *Lab Chip* 17 (2017) 2713–2739. <https://doi.org/10.1039/C7LC00397H>.
- [14] H. Kholafazad-Kordasht, M. Hasanazadeh, F. Seidi, Smartphone based immuno-sensors as next generation of physical activity tools: technical and analytical overview towards improvement of personalized medicine, *TrAC, Trends Anal. Chem.* 145 (2021), 116455. <https://doi.org/10.1016/j.trac.2021.116455>.
- [15] J.L.D. Nelis, A.S. Tsagkaris, M.J. Dillon, J. Hajslova, C.T. Elliott, Smartphone-based optical assays in the food safety field, *TrAC, Trends Anal. Chem.* 129 (2020). <https://doi.org/10.1016/j.trac.2020.115934>.
- [16] G.M.S. Ross, M.G.E.G. Bremer, M.W.F. Nielen, Consumer-friendly food allergen detection: moving towards smartphone-based immunoassays, *Anal. Bioanal. Chem.* 410 (2018). <https://doi.org/10.1007/s00216-018-0989-7>.
- [17] S. Jafari, J. Guercetti, A. Geballa-Koukoulia, A.S. Tsagkaris, J.L.D. Nelis, M.-P. Marco, J.-P. Salvador, A. Gerssen, J. Hajslova, C. Elliott, K. Campbell, D. Migliorelli, L. Burr, S. Generelli, M.W.F. Nielen, S.J. Sturla, ASSURED point-of-need food safety screening: a critical assessment of portable food analyzers, *Foods* 10 (2021) 1399. <https://doi.org/10.3390/foods10061399>.
- [18] M. Díaz-González, C. Fernández-Sánchez, Decentralized analysis of water contaminants using compact (bio)electroanalytical tools, *Curr Opin Environ Sci Health* 10 (2019) 47–56. <https://doi.org/10.1016/j.coesh.2019.08.003>.
- [19] B. Purohit, A. Kumar, K. Mahato, P. Chandra, Smartphone-assisted personalized diagnostic devices and wearable sensors, *Curr Opin Biomed Eng* 13 (2020) 42–50. <https://doi.org/10.1016/j.cobme.2019.08.015>.
- [20] K.J. Merazzo, J. Totoricaguena-Gorriño, E. Fernández-Martín, F.J. del Campo, E. Baldrich, Smartphone-enabled personalized diagnostics: current status and future prospects, *Diagnostics* 11 (2021) 1067. <https://doi.org/10.3390/diagnostics11061067>.
- [21] A.C. Sun, D.A. Hall, Point-of-Care smartphone-based electrochemical biosensing, *Electroanalysis* 31 (2019) 2–16. <https://doi.org/10.1002/elan.201800474>.
- [22] M. Rezazadeh, S. Seidi, M. Lid, S. Pedersen-Bjergaard, Y. Yamini, The modern role of smartphones in analytical chemistry, *TrAC, Trends Anal. Chem.* 118 (2019). <https://doi.org/10.1016/j.trac.2019.06.019>.
- [23] G.M. Fernandes, W.R. Silva, D.N. Barreto, R.S. Lamarca, P.C.F. Lima Gomes, J. Flávio da S Petrucci, A.D. Batista, Novel approaches for colorimetric measurements in analytical chemistry – a review, *Anal. Chim. Acta* 1135 (2020) 187–203. <https://doi.org/10.1016/j.aca.2020.07.030>.
- [24] Y.-H. Shin, M. Teresa Gutierrez-Wing, J.-W. Choi, Review - recent progress in portable fluorescence sensors, *J. Electrochem. Soc.* 168 (2021), 017502. <https://doi.org/10.1149/1945-7111/abd494>.
- [25] M. Mauk, J. Song, C. Liu, H. Bau, Simple approaches to minimally-instrumented, microfluidic-based point-of-care nucleic acid amplification tests, *Biosensors* 8 (2018) 17. <https://doi.org/10.3390/bios8010017>.
- [26] J.-F. Masson, Portable and field-deployed surface plasmon resonance and plasmonic sensors, *Analyst* 145 (2020). <https://doi.org/10.1039/D0AN00316F>.
- [27] A. Ozcan, Mobile phones democratize and cultivate next-generation imaging, diagnostics and measurement tools, *Lab Chip* 14 (2014) 3187–3194. <https://doi.org/10.1039/C4LC00010B>.
- [28] M.R. Bhalla, A.V. Bhalla, Generations of mobile wireless technology: a survey, *Int. J. Comput. Appl.* 5 (2010) 26–32. <https://doi.org/10.5120/905-1282>.
- [29] Samsung, <https://www.samsung.com/uk/mobile-phone-buying-guide/how-much-memory/>, (n.d.).
- [30] W. Easttom, *Modern Cryptography*, Springer International Publishing, Cham, 2021. <https://doi.org/10.1007/978-3-030-63115-4>.
- [31] Z. Guo, Y. Kang, S. Liang, J. Zhang, Detection of Hg(II) in adsorption experiment by a lateral flow biosensor based on streptavidin-biotinylated DNA probes modified gold nanoparticles and smartphone reader, *Environ. Pollut.* 266 (2020), 115389. <https://doi.org/10.1016/j.envpol.2020.115389>.
- [32] W. Luo, J. Deng, J. He, Z. Han, C. Huang, Y. Li, Q. Fu, H. Chen, A smartphone-based multi-wavelength photometer for on-site detection of the liquid colorimetric assays for clinical biochemical analyses, *Sensor. Actuator. B Chem.* 329 (2021), 129266. <https://doi.org/10.1016/j.snb.2020.129266>.
- [33] X. Li, J. Li, J. Ling, C. Wang, Y. Ding, Y. Chang, N. Li, Y. Wang, J. Cai, A smartphone-based bacteria sensor for rapid and portable identification of forensic saliva sample, *Sensor. Actuator. B Chem.* 320 (2020), 128303. <https://doi.org/10.1016/j.snb.2020.128303>.
- [34] Z. Li, Y. Cheng, K. Tang, Y. Xu, D. Zhang, A salt & pepper noise filter based on local and global image information, *Neurocomputing* 159 (2015) 172–185. <https://doi.org/10.1016/j.neucom.2014.12.087>.
- [35] J. Gu, R. Ramamoorthi, P. Belhumeur, S. Nayar, Removing image artifacts due to dirty camera lenses and thin occluders, *ACM Trans. Graph.* 28 (2009) 1–10. <https://doi.org/10.1145/1618452.1618490>.
- [36] G. Chen, Q. Wang, Y. Fan, Y. Han, Y. Wang, B. Urch, F. Silverman, M. Tian, Y. Su, X. Qiu, T. Zhu, A.W.H. Chan, Improved method for the optical analysis of particulate black carbon (BC) using smartphones, *Atmos. Environ.* 224 (2020), 117291. <https://doi.org/10.1016/j.atmosenv.2019.117291>.
- [37] Y. Zhao, C. Elliott, H. Zhou, K. Rafferty, Spectral illumination correction: achieving relative color constancy under the spectral domain, in: 2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), IEEE, 2018, pp. 690–695. <https://doi.org/10.1109/ISSPIT.2018.8642637>.
- [38] H.C. Karaim, M.S. Brown, A software platform for manipulating the camera imaging pipeline, *European Conference on Computer Vision*, https://doi.org/10.1007/978-3-319-46448-0_26, 2016.
- [39] L. Li, S. Jin, Y. Wang, Y. Liu, S. Shen, M. Li, Z. Ma, J. Ning, Z. Zhang, Potential of smartphone-coupled micro NIR spectroscopy for quality control of green tea, *Spectrochim. Acta Mol. Biomol. Spectrosc.* 247 (2021), 119096. <https://doi.org/10.1016/j.saa.2020.119096>.
- [40] L. Li, Y. Wang, S. Jin, M. Li, Q. Chen, J. Ning, Z. Zhang, Evaluation of black tea by using smartphone imaging coupled with micro-near-infrared spectrometer, *Spectrochim. Acta Mol. Biomol. Spectrosc.* 246 (2021), 118991. <https://doi.org/10.1016/j.saa.2020.118991>.
- [41] W. Xiao, C. Huang, F. Xu, J. Yan, H. Bian, Q. Fu, K. Xie, L. Wang, Y. Tang, A simple and compact smartphone-based device for the quantitative readout of colloidal gold lateral flow immunoassay strips, *Sensor. Actuator. B Chem.* 266 (2018) 63–70. <https://doi.org/10.1016/j.snb.2018.03.110>.
- [42] T. Gou, J. Hu, W. Wu, X. Ding, S. Zhou, W. Fang, Y. Mu, Smartphone-based mobile digital PCR device for DNA quantitative analysis with high accuracy, *Biosens. Bioelectron.* 120 (2018) 144–152. <https://doi.org/10.1016/j.bios.2018.08.030>.
- [43] O. Burggraaf, N. Schmidt, J. Zamorano, K. Pauly, S. Pascual, C. Tapia, E. Spyrales, F. Snik, Standardized spectral and radiometric calibration of consumer cameras, *Opt. Express* 27 (2019) 19075. <https://doi.org/10.1364/OE.27.019075>.
- [44] Y. Yao, C. Jiang, J. Ping, Flexible freestanding graphene paper-based potentiometric enzymatic aptasensor for ultrasensitive wireless detection of kanamycin, *Biosens. Bioelectron.* 123 (2019) 178–184. <https://doi.org/10.1016/j.bios.2018.08.048>.
- [45] D. Ji, Z. Liu, L. Liu, S. Shin Low, Y. Lu, X. Yu, L. Zhu, C. Li, Q. Liu, Smartphone-based integrated voltammetry system for simultaneous detection of ascorbic acid, dopamine, and uric acid with graphene and gold nanoparticles modified screen-printed electrodes, *Biosens. Bioelectron.* 119 (2018). <https://doi.org/10.1016/j.bios.2018.07.074>.
- [46] T. Fujimoto, S. Kawahara, Y. Fuchigami, S. Shimokawa, Y. Nakamura, K. Fukayama, M. Kamahori, S. Uno, Portable electrochemical sensing system attached to smartphones and its incorporation with paper-based electrochemical glucose sensor, *Int. J. Electr. Comput. Eng.* 7 (2017) 1423–1429. <https://doi.org/10.11591/ijece.v7i3.pp1423-1429>.
- [47] H.W. Jiang, A. Sun, A.G. Venkatesh, D.A. Hall, An audio jack-based electrochemical impedance spectroscopy, *Sensor for Point-of-Care Diagnostics* 17 (2017) 589–597. <https://doi.org/10.1109/JSEN.2016.2634530>.
- [48] Z. Liu, Q. Hua, J. Wang, Z. Liang, J. Li, J. Wu, X. Shen, H. Lei, X. Li, A smartphone-based dual detection mode device integrated with two lateral flow immunoassays for multiplex mycotoxins in cereals, *Biosens. Bioelectron.* 158 (2020). <https://doi.org/10.1016/j.bios.2020.112178>.

- [49] R. Wang, G. Ruan, Y. Sun, D. Zhao, H. Yu, C.-W. Zhang, L. Li, J. Liu, A full-wavelength coverage colorimetric sensor depending on polymer-carbon nanodots from blue to red for visual detection of nitrite via smartphone, *Dyes Pigments* 191 (2021), 109383. <https://doi.org/10.1016/j.dyepig.2021.109383>.
- [50] D.W. Raimundo, A. Ignatov, R. Timofte, LAN: Lightweight Attention-based Network for RAW-to-RGB Smartphone Image Processing, in: 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2022, pp. 807–815. <https://doi.org/10.1109/CVPRW56347.2022.00096>.
- [51] T.C.L. de Carvalho, C.A. Nunes, Smartphone-based method for the determination of chlorophyll and carotenoid contents in olive and avocado oils: an approach with calibration transfer, *J. Food Compos. Anal.* 104 (2021), 104164. <https://doi.org/10.1016/j.jfca.2021.104164>.
- [52] Y. Jung, Y. Heo, J.J. Lee, A. Deering, E. Bae, Smartphone-based lateral flow imaging system for detection of food-borne bacteria *E. coli* O157:H7, *J. Microbiol. Methods* 168 (2020). <https://doi.org/10.1016/j.mimet.2019.105800>.
- [53] Y. Zhang, Q. Luo, K. Ding, S.G. Liu, X. Shi, A smartphone-integrated colorimetric sensor of total volatile basic nitrogen (TVB-N) based on Au@MnO₂ core-shell nanocomposites incorporated into hydrogel and its application in fish spoilage monitoring, *Sensor. Actuator. B Chem.* 335 (2021), 129708. <https://doi.org/10.1016/j.snb.2021.129708>.
- [54] Y. Zhao, S.Y. Choi, J. Lou-Franco, J.L.D. Nelis, H. Zhou, C. Cao, K. Campbell, C. Elliott, K. Rafferty, Smartphone modulated colorimetric reader with color subtraction, 2019 IEEE Sensors (2019) 1–4. <https://doi.org/10.1109/SENSOR543011.2019.8956565>.
- [55] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A survey on the adoption of blockchain in IoT: challenges and solutions, *Blockchain: Res. Appl.* 2 (2021), 100006. <https://doi.org/10.1016/j.bcr.2021.100006>.
- [56] T. Li, A.K. Sahu, A. Talwalkar, V. Smith, Federated learning: challenges, methods, and future directions, *IEEE Signal Process. Mag.* 37 (2020) 50–60. <https://doi.org/10.1109/MSP.2020.2975749>.
- [57] V.D. Nguyen, H.Q. Nguyen, K.H. Bui, Y.S. Ko, B.J. Park, T.S. Seo, A handheld-type total integrated capillary electrophoresis system for SARS-CoV-2 diagnostics: power, fluorescence detection, and data analysis by smartphone, *Biosens. Bioelectron.* 195 (2022), 113632. <https://doi.org/10.1016/j.bios.2021.113632>.
- [58] J. Baranwal, B. Barse, G. Gatto, G. Broncova, A. Kumar, Electrochemical sensors and their applications: a review, *Chemosensors* 10 (2022) 363. <https://doi.org/10.3390/chemosensors10090363>.
- [59] Y. Yao, C. Jiang, J. Ping, Flexible freestanding graphene paper-based potentiometric enzymatic aptasensor for ultrasensitive wireless detection of kanamycin, *Biosens. Bioelectron.* 123 (2019) 178–184. <https://doi.org/10.1016/j.bios.2018.08.048>.
- [60] D. Zhang, Y. Lu, Q. Zhang, L. Liu, S. Li, Y. Yao, J. Jiang, G.L. Liu, Q. Liu, Protein detecting with smartphone-controlled electrochemical impedance spectroscopy for point-of-care applications, *Sens. Actuators B: Chem.* 222 (2016) 994–1002. <https://doi.org/10.1016/j.snb.2015.09.041>.
- [61] A.C. Sun, C. Yao, V. A.G. D.A. Hall, An efficient power harvesting mobile phone-based electrochemical biosensor for point-of-care health monitoring, *Sensor. Actuator. B Chem.* 235 (2016) 126–135. <https://doi.org/10.1016/j.snb.2016.05.010>.
- [62] A. Ainla, M.P.S. Mousavi, M.-N. Tsaloglou, J. Redston, J.G. Bell, M. Teresa Fernandez-Abedul, G.M. Whitesides, Open-source potentiostat for wireless electrochemical detection with smartphones, *Anal. Chem.* 90 (2018) 6240–6246. <https://doi.org/10.1021/acs.analchem.8b00850>.
- [63] V. Caratelli, S. Fillo, N. D'Amore, O. Rossetto, M. Pirazzini, M. Moccia, C. Avitabile, D. Moscone, F. Lista, F. Arduini, Paper-based electrochemical peptide sensor for on-site detection of botulinum neurotoxin serotype A and C, *Biosens. Bioelectron.* 183 (2021). <https://doi.org/10.1016/j.bios.2021.113210>.
- [64] Z. Zhao, L. Wei, M. Cao, M. Lu, A smartphone-based system for fluorescence polarization assays, *Biosens. Bioelectron.* 128 (2019) 91–96. <https://doi.org/10.1016/j.bios.2018.12.031>.
- [65] V.R. Pereira, B.S. Hosker, Low-cost (€5), open-source, potential alternative to commercial spectrophotometers, *PLoS Biol.* 17 (2019), e3000321. <https://doi.org/10.1371/journal.pbio.3000321>.
- [66] Y.M. Park, Y.D. Han, H.J. Chun, H.C. Yoon, Ambient light-based optical biosensing platform with smartphone-embedded illumination sensor, *Biosens. Bioelectron.* 93 (2017) 205–211. <https://doi.org/10.1016/j.bios.2016.09.007>.
- [67] C.S. Costa, E.C. Tetila, G. Astolfi, D.A. Sant'Ana, M.C. Brito Pacheco, A.B. Gonçalves, V.A. Garcia Zanoni, H.H. Picoli Nucci, O. Diemer, H. Pistori, A computer vision system for oocyte counting using images captured by smartphone, *Aquacult. Eng.* 87 (2019), 102017. <https://doi.org/10.1016/j.aquaeng.2019.102017>.
- [68] B. Coleman, C. Coarsey, M.A. Kabir, W. Asghar, Point-of-care colorimetric analysis through smartphone video, *Sensor. Actuator. B Chem.* 282 (2019) 225–231. <https://doi.org/10.1016/j.snb.2018.11.036>.
- [69] G.M.S. Ross, D. Filippini, M.W.F. Nielen, G.I.J. Salentijn, Unraveling the hook effect: a comprehensive study of high antigen concentration effects in sandwich lateral flow immunoassays, *Anal. Chem.* 92 (2020) 15587–15595. <https://doi.org/10.1021/acs.analchem.0c03740>.
- [70] E.G. Rey, D. O'Dell, S. Mehta, D. Erickson, Mitigating the hook effect in lateral flow sandwich immunoassays using real-time reaction kinetics, *Anal. Chem.* 89 (2017) 5095–5100. <https://doi.org/10.1021/acs.analchem.7b00638>.
- [71] K. He, X. Chen, S. Xie, Y. Li, P. Dollár, R. Girshick, Masked Autoencoders Are Scalable Vision Learners. <https://doi.org/10.48550/arXiv.2111.06377>, 2021. arxiv.org.
- [72] H.C. Koydemir, S. Rajpal, E. Gumustekin, D. Karınca, K. Liang, Z. Gorocs, D. Tseng, A. Ozcan, Smartphone-based turbidity reader, *Sci. Rep.* 9 (2019), 19901. <https://doi.org/10.1038/s41598-019-56474-z>.
- [73] B. Brandoli, G. Spadon, T. Esau, P. Hennessy, A.C.P.L. Carvalho, S. Amer-Yahia, J.F. Rodrigues Jr., DropLeaf: a precision farming smartphone tool for real-time quantification of pesticide application coverage, *Comput. Electron. Agric.* 180 (2021), 105906. <https://doi.org/10.1016/j.compag.2020.105906>.
- [74] G.M.S. Ross, D. Filippini, M.W.F. Nielen, G.I.J. Salentijn, Interconnectable solid-liquid protein extraction unit and chip-based dilution for multiplexed consumer immunodiagnoses, *Anal. Chim. Acta.* 1140 (2020) 190–198. <https://doi.org/10.1016/j.aca.2020.1018>.
- [75] A. Geballa-Koukoulou, A. Gerssen, M.H. Blokland, C.T. Elliott, J. Pawliszyn, M.W.F. Nielen, Immuno-enriched microspheres - magnetic blade spray-tandem mass spectrometry for domoic acid in mussels, *Anal. Chem.* 93 (2021) 15736–15743. <https://doi.org/10.1021/acs.analchem.1c03816>.
- [76] Y. Chen, Q. Fu, D. Li, J. Xie, D. Ke, Q. Song, Y. Tang, H. Wang, A smartphone colorimetric reader integrated with an ambient light sensor and a 3D printed attachment for on-site detection of zearalenone, *Anal. Bioanal. Chem.* 409 (2017) 6567–6574. <https://doi.org/10.1007/s00216-017-0605-2>.
- [77] Y. Man, A. Li, B. Li, J. Liu, L. Pan, A microfluidic colorimetric immunoassay for sensitive detection of altenarol monomethyl ether by UV spectroscopy and smart phone imaging, *Anal. Chim. Acta* 1092 (2019) 75–84. <https://doi.org/10.1016/j.aca.2019.09.039>.
- [78] Nelis, Bura Zhao, Rafferty Burkin, Campbell Elliott, The efficiency of color space channels to quantify color and color intensity change in liquids, pH strips, and lateral flow assays with smartphones, *Sensors* 19 (2019) 5104. <https://doi.org/10.3390/s19235104>.
- [79] E. Aydinoglu, E. Gulur Celik, S. Timur, Paper-based analytical methods for smartphone sensing with functional nanoparticles: bridges from smart surfaces to global health, *Anal. Chem.* 90 (2018) 12325–12333. <https://doi.org/10.1021/acs.analchem.8b03120>.
- [80] A. Carter, J. Little, W. Hall, H. Chenery, Mobile phones in research and treatment: ethical guidelines and future directions, *JMIR Mhealth Uhealth* 3 (2015) e95. <https://doi.org/10.2196/mhealth.4538>.
- [81] J. Lerner, J. Tirole, NATIONAL BUREAU OF ECONOMIC RESEARCH, The scope of open source licensing. <https://doi.org/10.3386/w9363>, 2002.
- [82] L. Saisin, R. Amarit, A. Sombonkaew, O. Gajanandana, O. Himananto, B. Sutapun, Significant sensitivity improvement for camera-based lateral flow immunoassay readers, *Sensors* 18 (2018) 4026. <https://doi.org/10.3390/s18114026>.
- [83] C. Grazioli, G. Faura, N. Dossi, R. Toniolo, M. Abate, F. Terzi, G. Bontempelli, 3D printed portable instruments based on affordable electronics, smartphones and open-source microcontrollers suitable for monitoring food quality, *Microchem. J.* 159 (2020), 105584. <https://doi.org/10.1016/j.microc.2020.105584>.
- [84] T.F. Fernandez, M. Pradeep, M. Adetunji, R.E. Fernandez, Hardware–software interfacing in smartphone centered biosensing, in: *Micro- and Nanotechnology Enabled Applications for Portable Miniaturized Analytical Systems*, Elsevier, 2022, pp. 401–412. <https://doi.org/10.1016/B978-0-12-823727-4.00017-1>.
- [85] R. Ahmad, et al., KAUSTat: a wireless, wearable, open-source potentiostat for electrochemical measurements, 2019 IEEE Sensors (2019) 1–4. <https://doi.org/10.1109/SENSOR543011.2019.8956815>.
- [86] G.F. Giordano, M.B.R. Vicentini, R.C. Murer, F. Augusto, M.F. Ferrão, G.A. Helfer, A.B. da Costa, A.L. Gobbi, L.W. Hantao, R.S. Lima, M.F. Ferrao, Point-of-use electroanalytical platform based on homemade potentiostat and smartphone for multivariate data processing, *Electrochim. Acta.* 219 (2016). <https://doi.org/10.1016/j.electacta.2016.09.157>.
- [87] D.M. Jenkins, B.E. Lee, S. Jun, J. Reyes-De-Corcuera, E.S. McLamore, ABE-stat, a fully open-source and versatile wireless potentiostat project including electrochemical impedance spectroscopy, *J. Electrochem. Soc.* 166 (2019) B3056–B3065. <https://doi.org/10.1149/2.0061909jes>.
- [88] A. Das, S. Bose, N. Mandal, B. Pramanick, C. RoyChaudhuri, HOME-Stat: a handheld potentiostat with open-access mobile-interface and extended measurement ranges, *Proc. Indian Nat. Sci. Acad.* 87 (2021) 84–93. <https://doi.org/10.1007/s43538-021-00008-7>.
- [89] C. Mercer, R. Bennett, P.O. Conghaile, J.F. Rusling, D. Leech, Glucose biosensor based on open-source wireless microfluidic potentiostat, *Sens. Actuators B: Chem.* 290. <https://doi.org/10.1016/j.snb.2019.02.031>.
- [90] PalmSens, PalmSens Compact Electrochemical Interfaces, <https://www.palmsens.com/>, (n.d.).
- [91] M. Ebner, Color constancy, *Color. Technol.* 125 (2009) 366–367. <https://doi.org/10.1111/j.1478-4408.2009.00219.x>.
- [92] D. Omanović, C. Garnier, Y. Louis, V. Lenoble, S. Mounier, I. Pizeta, Significance of data treatment and experimental setup on the determination of copper complexing parameters by anodic stripping voltammetry, *Anal. Chim. Acta* 664 (2010) 136–143. <https://doi.org/10.1016/j.aca.2010.02.008>.
- [93] F. Šroubek, J. Kamenický, J. Flusser, in: C.A. Bouman, I. Pollak, P.J. Wolfe (Editors), Denoising, Deblurring, and Superresolution in Mobile Phones, 2011, p. 787301. <https://doi.org/10.1117/12.872577>.
- [94] ISO, ISO 17321-1:2012 Graphic Technology and Photography - Colour

- Characterisation of Digital Still Cameras (DSCs) - Part 1: Stimuli, Metrology and Test Procedures, International Organization for Standardization, 2017. <https://www.iso.org/standard/56537.html>.
- [95] O. Burggraaff, A.B. Perduijn, R.F. van Hek, N. Schmidt, C.U. Keller, F. Snik, A universal smartphone add-on for portable spectroscopy and polarimetry: iSPEX 2, in: M.S. Islam, T. George (Editors), Micro- and Nanotechnology Sensors, Systems, and Applications XII, SPIE, 2020, p. 95. <https://doi.org/10.1117/12.2558562>.
- [96] M. Wang, X. Liu, Y. Gao, X. Ma, N.Q. Soomro, Superpixel segmentation: a benchmark, *Signal Process. Image Commun.* 56 (2017) 28–39. <https://doi.org/10.1016/j.image.2017.04.007>.
- [97] M.S. Woolf, L.M. Dignan, A.T. Scott, J.P. Landers, Digital postprocessing and image segmentation for objective analysis of colorimetric reactions, *Nat. Protoc.* 16 (2021) 218–238. <https://doi.org/10.1038/s41596-020-00413-0>.
- [98] G.M.S. Ross, M.G.E.G. Bremer, J.H. Wichers, A. van Amerongen, M.W.F. Nielen, Rapid antibody selection using surface plasmon resonance for high-speed and sensitive hazelnut lateral flow prototypes, *Biosensors* 8 (2018). <https://doi.org/10.3390/bios8040130>.
- [99] Y. Man, M. Ban, A.A.A. Li, X. Jin, Y. Du, L. Pan, A microfluidic colorimetric biosensor for in-field detection of Salmonella in fresh-cut vegetables using thiolated polystyrene microspheres, hose-based microvalve and smartphone imaging APP, *Food Chem.* 354 (2021), 129578. <https://doi.org/10.1016/j.foodchem.2021.129578>.
- [100] Q. Li, T. Sun, G.I.J. Salentijn, B. Ning, D. Han, J. Bai, Y. Peng, Z. Gao, Z. Wang, Bifunctional ligand-mediated amplification of polydiacetylene response to biorecognition of diethylstilbestrol for on-site smartphone detection, *J. Hazard Mater.* 432 (2022), 128692. <https://doi.org/10.1016/j.jhazmat.2022.128692>.
- [101] H. Li, P. Dauphin-Ducharme, G. Ortega, K.W. Plaxco, Calibration-free electrochemical biosensors supporting accurate molecular measurements directly in undiluted whole blood, *J. Am. Chem. Soc.* 139 (2017) 11207–11213. <https://doi.org/10.1021/jacs.7b05412>.
- [102] Y. Zhao, S. Ferguson, H. Zhou, C. Elliott, K. Rafferty, Color alignment for relative color constancy via non-standard references, *IEEE Trans. Image Process.* 31 (2022) 6591–6604. <https://doi.org/10.1109/TIP.2022.3214107>.
- [103] M. Nixon, F. Outlaw, T.S. Leung, Accurate device-independent colorimetric measurements using smartphones, *PLoS One* 15 (2020), e0230561. <https://doi.org/10.1371/journal.pone.0230561>.
- [104] S.D. Kim, Y. Koo, Y. Yun, A smartphone-based automatic measurement method for colorimetric pH detection using a color adaptation algorithm, *Sensors* 17 (2017) 1604. <https://doi.org/10.3390/s17071604>.
- [105] C. Morikawa, M. Kobayashi, M. Satoh, Y. Kuroda, T. Inomata, H. Matsuo, T. Miura, M. Hilaga, Image and video processing on mobile devices: a survey, *Vis. Comput.* 37 (2021) 2931–2949. <https://doi.org/10.1007/s00371-021-02200-8>.
- [106] R.M. Haralick, L.G. Shapiro, Image segmentation techniques, *Comput. Vis. Graph Image Process* 29 (1985) 100–132. [https://doi.org/10.1016/S0734-189X\(85\)90153-7](https://doi.org/10.1016/S0734-189X(85)90153-7).
- [107] M.-Y. Pan, K.-L. Lee, S.-C. Lo, P.-K. Wei, Resonant position tracking method for smartphone-based surface plasmon sensor, *Anal. Chim. Acta* 1032 (2018) 99–106. <https://doi.org/10.1016/j.aca.2018.05.033>.
- [108] T. Hou, H. Chang, H. Jiang, P. Wang, N. Li, Y. Song, D. Li, Smartphone based microfluidic lab-on-chip device for real-time detection, counting and sizing of living algae, *Measurement* 187 (2022), 110304. <https://doi.org/10.1016/j.measurement.2021.110304>.
- [109] M. Jakubowska, Signal processing in electrochemistry, *Electroanalysis* (2011). <https://doi.org/10.1002/elan.201000465>.
- [110] J. Cai, J. Luo, S. Wang, S. Yang, Feature selection in machine learning: a new perspective, *Neurocomputing* 300 (2018) 70–79. <https://doi.org/10.1016/j.neucom.2017.11.077>.
- [111] G. Chandrashekar, F. Sahin, A survey on feature selection methods, *Comput. Electr. Eng.* 40 (2014) 16–28. <https://doi.org/10.1016/j.compeleceng.2013.11.024>.
- [112] H. Ceylan Koydemir, S. Rajpal, E. Gumustekin, D. Karinca, K. Liang, Z. Göröcs, D. Tseng, A. Ozcan, Smartphone-based turbidity reader, *Sci. Rep.* 9 (2019), 19901. <https://doi.org/10.1038/s41598-019-56474-z>.
- [113] U. Barman, R.D. Choudhury, Smartphone assist deep neural network to detect the citrus diseases in agri-informatics, *Glob. Transit. Proc.* (2021). <https://doi.org/10.1016/j.gltp.2021.10.004>.
- [114] E.C. Rivera, J.J. Swerdlow, R.L. Summerscales, P.P.T. Uppala, R. Maciel Filho, M.R.C. Neto, H.J. Kwon, R. Maciel, M.R.C. Neto, H.J. Kwon, Data-driven modeling of smartphone-based electrochemiluminescence sensor data using artificial intelligence, *Sensors* 20 (2020). <https://doi.org/10.3390/s20030625>.
- [115] K. Lee, Y. Wang, W. Wei, M. Chiang, T. Dai, C. Pan, T. Chen, S. Luo, P. Li, J. Chen, S. Liaw, C. Lin, C. Wu, J. Chieh, An optical smartphone-based inspection platform for identification of diseased orchids, *Biosensors* 11 (2021) 363. <https://doi.org/10.3390/bios11100363>.
- [116] J. Müller-Maatsch, F.R. Bertani, A. Mencattini, A. Gerardino, E. Martinelli, Y. Weesepoel, S. van Ruth, The spectral treasure house of miniaturized instruments for food safety, quality and authenticity applications: a perspective, *Trends Food Sci. Technol.* 110 (2021) 841–848. <https://doi.org/10.1016/j.tifs.2021.01.091>.
- [117] A. Soni, R.K. Surana, S.K. Jha, Smartphone based optical biosensor for the detection of urea in saliva, *Sensor. Actuator. B Chem.* 269 (2018) 346–353. <https://doi.org/10.1016/j.snb.2018.04.108>.
- [118] S. Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System, 2008. www.bitcoin.org.
- [119] P. Sandner, J. Gross, R. Richter, Convergence of blockchain, IoT, and AI, *Front. Blockchain* 3 (2020). <https://doi.org/10.3389/fbloc.2020.522600>.
- [120] D.R. Wong, S. Bhattacharya, A.J. Butte, Prototype of running clinical trials in an untrustworthy environment using blockchain, *Nat. Commun.* 10 (2019) 917. <https://doi.org/10.1038/s41467-019-08874-y>.
- [121] F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, P. Menesatti, A review on blockchain applications in the agri-food sector, *J. Sci. Food Agric.* 99 (2019) 6129–6138. <https://doi.org/10.1002/jsfa.9912>.
- [122] Y. Cao, F. Jia, G. Manogaran, Efficient traceability systems of steel products using blockchain-based industrial internet of Things, *IEEE Trans. Ind. Inf.* 16 (2020) 6004–6012. <https://doi.org/10.1109/TII.2019.2942211>.
- [123] M.J.M. Chowdhury, A. Colman, M.A. Kabir, J. Han, P. Sarda, Blockchain versus database: a critical analysis, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, IEEE, 2018, pp. 1348–1353.
- [124] L. Hickey, M. Harrigan, The Bisq decentralised exchange: on the privacy cost of participation, *Blockchain: Res. Appl.* 3 (2022), 100029. <https://doi.org/10.1016/j.bcr.2021.100029>.
- [125] Y.-A. de Montjoye, S. Gams, V. Blondel, G. Canright, N. de Cordes, S. Deletaille, K. Engö-Monsen, M. Garcia-Herranz, J. Kendall, C. Kerry, G. Krings, E. Letouze, M. Luengo-Oroz, N. Oliver, L. Rocher, A. Rutherford, Z. Smoreda, J. Steele, E. Wetter, A. Sandy Pentland, L. Bengtsson, On the privacy-conscious use of mobile phone data, *Sci. Data* 5 (2018) 1–5. <https://doi.org/10.1038/sdata.2018.286> (2018) 1–6.
- [126] N. Oliver, B. Lepri, H. Sterly, R. Lambiotte, S. Deletaille, M. de Nadai, E. Letouze, A.A. Salah, R. Benjamins, C. Cattuto, V. Colizza, N. de Cordes, S.P. Fraiberger, T. Koebe, S. Lehmann, J. Murillo, A. Pentland, P.N. Pham, F. Pivetta, J. Saramäki, S. v. Scarpino, M. Tizzoni, S. Verhulst, P. Vinck, Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle, *Sci. Adv.* 6 (2020). <https://doi.org/10.1126/sciadv.abc0764>.
- [127] European Convention for the Protection of Human Rights and Fundamental Freedoms, Sept. 3, 1953, ETS 5, 213 UNTS 221, (n.d.).
- [128] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, ((n.d.)).
- [129] European Commission, Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, *Official Journal of European Union*, 1997, 0001–0008.
- [130] European Commission, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, (n.d.).
- [131] European Commission, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), L 201, *Official Journal of European Union*, 2002, 0037–0047.
- [132] European Union, The Charter of Fundamental Rights of the European Union, *Official Journal of the European Union* C83, 53, European Union, 2012. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.
- [133] M. Mostert, A.L. Bredenoord, B. van der Sloot, J.J.M. van Delden, From privacy to data protection in the eu: implications for big data health research, *Eur. J. Health Law* 25 (2018) 43–55. <https://doi.org/10.1163/15718093-12460346>.
- [134] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, (n.d.).
- [135] C. Ryngaert, M. Taylor, The GDPR as global data protection regulation? *Am. J. Int. Law* 114 (2020) 5–9. <https://doi.org/10.1017/AJIL.2019.80>.
- [136] S. Gerke, C. Shachar, P.R. Chai, I.G. Cohen, Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19, *Nat. Med.* 26 (2020) 1176–1182. <https://doi.org/10.1038/s41591-020-0994-1>.
- [137] R. Holzer, W. Bloch, C. Brinkmann, Minimally invasive electrochemical patch-based sensor system for monitoring glucose and lactate in the human body-A survey-based analysis of the end-user's perspective, *Sensors* 20 (2020). <https://doi.org/10.3390/s20205761>.
- [138] M.L. Zigman Suchsland, I. Rahmatullah, B. Lutz, V. Lyon, S. Huang, E. Kline, C. Graham, S. Cooper, P. Su, S. Smedinghoff, H.Y. Chu, K. Sewalk, J.S. Brownstein, M.J. Thompson, Evaluating an app-guided self-test for influenza: lessons learned for improving the feasibility of study designs to evaluate self-tests for respiratory viruses, *BMC Infect. Dis.* 21 (2021). <https://doi.org/10.1186/S12879-021-06314-1>.
- [139] M.E. Villarreal, S.R. Villarreal, C. Westphall, J. Werner, Privacy token: an improved and verified mechanism for user's privacy specification in identity management systems for the cloud, *Int. J. Adv. Secur.* 10 (2017).
- [140] S.H. Browne, M. Bernstein, S.C. Pan, J. Gonzalez Garcia, C.A. Easson, C.-C.C. Huang, F. Vaida, J.G. Garcia, C.A. Easson, C.-C.C. Huang, F. Vaida, Smartphone biosensor with app meets FDA/ISO standards for clinical pulse oximetry and can be reliably used by a wide range of patients, *Chest* 159

- (2021).
- [141] J. Pavlas, O. Krejcar, P. Maresova, A. Selamat, Prototypes of user interfaces for mobile applications for patients with diabetes, *Computers* 8 (2018). <https://doi.org/10.3390/computers8010001>.
 - [142] D. Bakkiam Deebak, F. Al-Turjman, Lightweight privacy-aware secure authentication scheme for cyber-physical systems in the edge intelligence era, *Concurr. Comput.* (2021). <https://doi.org/10.1002/cpe.6510>.
 - [143] A. Bourla, F. Ferreri, L. Ogorzelec, C.-S.S. Peretti, C. Guinchard, S. Mouchabac, Psychiatrists' attitudes toward disruptive new technologies: mixed-methods study, *JMIR Ment Health* 5 (2018). <https://doi.org/10.2196/10240>.
 - [144] R. Kadam, W. White, N. Banks, Z. Katz, S. Dittrich, C. Kelly-Cirino, Target Product Profile for a mobile app to read rapid diagnostic tests to strengthen infectious disease surveillance, *PLoS One* 15 (2020). <https://doi.org/10.1371/journal.pone.0228311>.
 - [145] S. Mohammed, A. Shariff, M. Singh, An Authentication Technique: Behavioral Data Profiling on Smart Phones, in: R. Alfred, H. Iida, A. Ag. Ibrahim, Y. Lim (Editors), *Computational Science and Technology. ICCST 2017. Lecture Notes in Electrical Engineering*, 488, Springer, Singapore, 2018. https://doi.org/10.1007/978-981-10-8276-4_9.
 - [146] V. Pathak, A priority based efficient secure framework for WBANs, *Int. J. Inf. Secur. Priv.* 13 (2019) 60–73. <https://doi.org/10.4018/IJISP.201907010104>.
 - [147] N. Talebi, C. Hallam, G. Zanella, The new wave of privacy concerns in the wearable devices era, in: 2016 Portland International Conference on Management of Engineering and Technology, PICMET, 2016, pp. 3208–3214. <https://doi.org/10.1109/PICMET.2016.7806826>.
 - [148] C. Zajc, G. Holweg, C. Steger, System architecture and security issues of smartphone-based point-of-care devices, in: *Proceedings - Euromicro Conference on Digital System Design, DSD 2020*, 2020, pp. 320–324. <https://doi.org/10.1109/DSD51259.2020.00059>.
 - [149] Z.-G. Chen, H.-S. Kang, S.-N. Yin, S.-R. Kim, An efficient privacy protection in mobility social network services with novel clustering-based anonymization, *EURASIP J. Wirel. Commun. Netw.* (2016). <https://doi.org/10.1186/s13638-016-0767-1>, 2016.
 - [150] A. Reuter, A. Abdelmaksoud, K. Boudaoud, M. Winckler, Usability of end-to-end encryption in E-mail communication, *Front Big Data* 4 (2021) 42. <https://doi.org/10.3389/FDATA.2021.568284/BIBTEX>.
 - [151] T. Le, G. Salles-Loustau, P. Xie, Z. Lin, L. Najafizadeh, M. Javanmard, S. Zonouz, Trusted sensor signal protection for confidential point-of-care medical diagnostic, *IEEE Sensor. J.* 17 (2017) 5807–5816. <https://doi.org/10.1109/JSEN.2017.2732026>.
 - [152] R. Gupta, W.J. Peveler, K. Lix, W.R. Algar, Comparison of semiconducting polymer dots and semiconductor quantum dots for smartphone-based fluorescence assays, *Anal. Chem.* 91 (2019) 10955–10960. <https://doi.org/10.1021/acs.analchem.9b02881>.
 - [153] T. Le, G. Salles-Loustau, L. Najafizadeh, M. Javanmard, S. Zonouz, BioMEMS-based coding for secure medical diagnostic devices, in: 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE, 2016, pp. 4419–4422. <https://doi.org/10.1109/EMBC.2016.7591707>.
 - [154] D. Spichtinger, Data Management Plans in Horizon 2020: what beneficiaries think and what we can learn from their experience, *Open Res. Eur.* 1 (2021) 42. <https://doi.org/10.12688/OPENRESEUROPE.13342.1>.
 - [155] H. Zhu, L. Gao, H. Li, Secure and privacy-preserving body sensor data collection and query scheme, *Sensors* 16 (2016) 179. <https://doi.org/10.3390/S16020179>, 16 (2016) 179.
 - [156] W. Tang, K. Zhang, J. Ren, Y. Zhang, X. Shen, Flexible and efficient authenticated key agreement scheme for BANs based on physiological features, *IEEE Trans. Mobile Comput.* 18 (2019) 845–856. <https://doi.org/10.1109/TMC.2018.2848644>.
 - [157] N. Pai, A. Esmail, P.S. Chaudhuri, S. Oelofse, M. Pretorius, G. Marathe, J. Daher, M. Smallwood, N. Karatzas, M. Fadul, A. de Waal, N. Engel, A.A. Zwerling, K. Dheda, Impact of a personalised, digital, HIV self-testing app-based program on linkages and new infections in the township populations of South Africa, *BMJ Glob Health* 6 (2021), e006032. <https://doi.org/10.1136/BMJGH-2021-006032>.
 - [158] M. Shamim Hossain, G. Muhammad, Cloud-assisted industrial internet of Things (IIoT) - enabled framework for health monitoring, *Comput. Netw.* 101 10.1016/j.comnet.2016.01.009.
 - [159] G.B. R. B. A. K.K. K. S. Maurya, S.K. Saravana, Smartphone-based electrochemical sensor for assessing COVID-19 infected patients, *Int. J. Pervasive Comput. Commun.* 18 (5) (2020) 563–572. <https://doi.org/10.1108/IJPPC-10-2020-0169>.
 - [160] T. Cao, C. Carfano, G.A. Rodriguez, M.H. Choudhury, F.O. Afzal, S.M. Weiss, Porous silicon sensors: from on-chip to mobile diagnostics, in: *Progress in Biomedical Optics and Imaging - Proceedings of SPIE*, 2019. <https://doi.org/10.1117/12.2508685>.
 - [161] Y. Lin, J. Sun, M. Tang, G. Zhang, L. Yu, X. Zhao, R. Ai, H. Yu, B. Shao, Y.Y. He, Synergistic recognition-triggered charge transfer enables rapid visual colorimetric, *Detection of Fentanyl* 93 (2021) 6544–6550. <https://doi.org/10.1021/acs.analchem.1c00723>.
 - [162] P. Teengam, W. Siangproh, S. Tontisirin, A. Jiraseree-amornkun, N. Chuaypen, P. Tangkijvanich, C.S. Henry, Ngamrojanavanich, O. Chailapakul, NFC-enabling smartphone-based portable amperometric immunosensor for hepatitis B virus detection, *Sens. Actuators B: Chem.* 326 (2021). <https://doi.org/10.1016/j.snb.2020.128825>.
 - [163] M. Chmielewski, K. Sapiejewski, M. Sobolewski, Application of augmented reality, mobile devices, and sensors for a combat entity quantitative assessment supporting decisions and situational awareness development, *Appl. Sci.* 9 (2019) 4577. <https://doi.org/10.3390/app9214577>.
 - [164] L.-S. Yu, J. Rodriguez-Manzano, N. Moser, A. Moniri, K. Malpartida-Cardenas, N. Miscourides, T. Sewell, T. Kochina, A. Brackin, J. Rhodes, A.H. Holmes, M.C. Fisher, P. Georgiou, Rapid detection of azole-resistant *Aspergillus fumigatus* in clinical and environmental isolates by use of a lab-on-a-chip diagnostic system, *J. Clin. Microbiol.* 58 (2020). <https://doi.org/10.1128/JCM.00843-20>.
 - [165] C. Jin, Y. Bouzembrak, J. Zhou, Q. Liang, L.M. van den Bulk, A. Gavai, N. Liu, L.J. van den Heuvel, W. Hoenderdaal, H.J.P. Marvin, Big Data in food safety- A review, *Curr. Opin. Food Sci.* 36 (2020) 24–32. <https://doi.org/10.1016/J.COFS.2020.11.006>.
 - [166] J.P. Ku, I. Sim, Mobile Health: making the leap to research and clinics, *Npj Digit. Med.* 4 (2021) 1. <https://doi.org/10.1038/s41746-021-00454-z>, 4 (2021) 1–4.
 - [167] C. Jin, Y. Bouzembrak, J. Zhou, Q. Liang, L.M. van den Bulk, A. Gavai, N. Liu, L.J. van den Heuvel, W. Hoenderdaal, H.J.P. Marvin, Big Data in food safety- A review, *Curr. Opin. Food Sci.* 36 (2020) 24–32. <https://doi.org/10.1016/J.COFS.2020.11.006>.
 - [168] M. Ottaviano, M.E. Beltrán-Jaunsarás, J.G. Teriús-Padrón, R.I. García-Betances, S. González-Martínez, G. Cea, C. Vera, M.F. Cabrera-Umpiérrez, M.T.A. Waldmeyer, Empowering citizens through perceptual sensing of urban environmental and health data following a participative citizen science approach, *Sensors* 19 (2019) 2940. <https://doi.org/10.3390/S19132940>.
 - [169] Z. Geradts, Digital, big data and computational forensics, *Forensic Sci. Res.* 3 (2018) 179. <https://doi.org/10.1080/20961790.2018.1500078>.
 - [170] M. Rahlha, S. Allegue, T. Abdellatif, Guidelines for GDPR compliance in big data systems, *J. Inf. Secur. Appl.* 61 (2021), 102896. <https://doi.org/10.1016/J.JISA.2021.102896>.
 - [171] E. Anane-Sarpong, T. Wangmo, M. Tanner, Ethical principles for promoting health research data sharing with sub-Saharan Africa, *Develop. World Bioeth.* 20 (2020) 86–95. <https://doi.org/10.1111/DEWB.12233>.
 - [172] Nima Labs Inc. Privacy Policy, (n.d.). <https://blog.nimasensor.com/privacy-policy/> (accessed October 18, 2021).
 - [173] J. Starkbaum, U. Felt, Negotiating the reuse of health-data: Research, Big Data, and the European General Data Protection Regulation, *Big Data Soc.* 6 (2019). <https://doi.org/10.1177/2053951719862594>.
 - [174] E.S. McLamore, E. Alolija, C. Gomes, S. Gunasekaran, D. Jenkins, S.P.A. Datta, Y. Li, Y. Mao, S.R. Nugen, J.I. ReyesDeCorcuera, P. Takhistov, O. Tsyusko, J.P. Cochran, T.R. Tzeng, J.Y. Yoon, C. Yu, A. Zhou, FEAST of biosensors: food, environmental and agricultural sensing technologies (FEAST) in North America, *Biosens. Bioelectron.* 178 (2021). <https://doi.org/10.1016/j.bios.2021.113011>.
 - [175] E. Muravyeva, J. Janssen, K. Dirkx, M. Specht, Students' attitudes towards personal data sharing in the context of e-assessment: informed consent or privacy paradox? *Commun. Comput. Inform. Sci.* 1014 (2019) 16–26. https://doi.org/10.1007/978-3-030-25264-9_2.
 - [176] T. Lakshanasopin, T.W. Guo, S. Nayak, A.A. Sridhara, S. Xie, O.O. Olowookere, P. Cadinu, F. Meng, N.H. Chee, J. Kim, C.D. Chin, E. Munyazesa, P. Mugwaneza, A.J. Rai, V. Mugisha, A.R. Castro, D. Steinmiller, V. Linder, J.E. Justman, S. Nsanzimana, S.K. Sia, A smartphone dongle for diagnosis of infectious diseases at the point of care, *Sci. Transl. Med.* 7 (2015) 273re1. <https://doi.org/10.1126/scitranslmed.aaa0056>.
 - [177] I. Rasheed, L. Zhang, F. Hu, A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing, *Comput. Network.* 176 (2020). <https://doi.org/10.1016/j.comnet.2020.107283>.
 - [178] F. Maritsch, I. Cil, C. McKinnon, J. Potash, N. Baumgartner, V. Philippon, B.G. Pavlova, Data privacy protection in scientific publications: process implementation at a pharmaceutical company, *BMC Med. Ethics* 23 (2022) 65. <https://doi.org/10.1186/s12910-022-00804-w>.
 - [179] A. Fukami, R. Stoykova, Z. Geradts, A new model for forensic data extraction from encrypted mobile devices, *Forensic Sci. Int.: Digit. Invest.* 38 (2021), 301169. <https://doi.org/10.1016/j.fsi.2021.301169>.
 - [180] N.P. Owah, M.M. Singh, SenseCrypt: a security framework for mobile crowd sensing applications, *Sensors* 20 (2020) 3280. <https://doi.org/10.3390/S20113280>, 20 (2020) 3280.
 - [181] D. Hayes, F. Cappa, N.A. Le-Khac, An effective approach to mobile device management: security and privacy issues associated with mobile applications, *Digit. Bus.* 1 (2020), 100001. <https://doi.org/10.1016/j.digbus.2020.100001>.
 - [182] S. Iqbal, M.L. Mat Kiah, A. ur Rehman, Z. Abbas, B. Daghighi, DM-GKM: a key management scheme for dynamic group based applications, *Comput. Network.* 182 (2020), 107476. <https://doi.org/10.1016/j.comnet.2020.107476>.
 - [183] J. Picaut, A. Boumchich, E. Bocher, N. Fortin, G. Petit, P. Aumond, A smartphone-based crowd-sourced database for environmental noise assessment, *Int. J. Environ. Res. Publ. Health* 18 (2021). <https://doi.org/10.3390/IJERPH18157777>.
 - [184] S. Gupta, A. Burio, B. Crispo, Demystifying authentication concepts in smartphones: ways and types to secure access, *Mobile Inf. Syst.* (2018). <https://doi.org/10.1155/2018/2649598>.
 - [185] M. Shirvanian, N. Saxena, S. Jarecki, H. Krawczyk, Building and studying a password store that perfectly, *Hides Passwords from Itself* 16 (2019)

- 770–782. <https://doi.org/10.1109/TDSC.2019.2902551>.
- [186] A.E.B. Tomaz, J.C.D. Nascimento, A.S. Hafid, J.N. de Souza, Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain, *IEEE Access* 8 (2020) 204441–204458. <https://doi.org/10.1109/ACCESS.2020.3036811>.
- [187] H. Tan, I. Chung, Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor, *IEEE Access* 7 (2019) 151459–151474. <https://doi.org/10.1109/ACCESS.2019.2948207>.
- [188] M. Konan, W. Wang, A secure mutual batch authentication scheme for patient data privacy preserving in WBAN, *Sensors* 19 (2019). <https://doi.org/10.3390/s19071608>.
- [189] S. Kloppenburg, I. van der Ploeg, Securing identities: biometric technologies and the enactment of human bodily differences, *Sci. Cult.* 29 (2020) 57–76. <https://doi.org/10.1080/09505431.2018.1519534>.
- [190] S. Chandra Kishore, K. Samikannu, R. Atchudan, S. Perumal, T.N.J.I. Edison, M. Alagan, A.K. Sundramoorthy, Y.R. Lee, Smartphone-operated wireless chemical sensors: a review, *Chemosensors* 10 (2022) 55. <https://doi.org/10.3390/chemosensors10020055>.
- [191] S. Roy, N. Ghosh, P. Ghosh, S.K. Das, bioMCS, in: *Proceedings of the 21st International Conference on Distributed Computing and Networking*, ACM, New York, NY, USA, 2020, pp. 1–10. <https://doi.org/10.1145/3369740.3369788>.
- [192] J. van Hoboken, R.O. Fathaigh, Smartphone platforms as privacy regulators, *Comput. Law Secur. Rev.* 41 (2021). <https://doi.org/10.1016/j.clsr.2021.105557>.
- [193] M. Chung, I. Ko, Data-sharing method for multi-smart devices at close range, *Mobile Inf. Syst.* (2015) 1–11. <https://doi.org/10.1155/2015/931765>, 2015.
- [194] Z. Cao, P. Chen, Z. Ma, S. Li, X. Gao, R. Wu, L. Pan, Y. Shi, Near-field communication sensors, *Sensors* 19 (2019) 3947. <https://doi.org/10.3390/s19183947>.
- [195] R. Lin, H.-J. Kim, S. Achavananthadith, S.A. Kurt, S.C.C. Tan, H. Yao, B.C.K. Tee, J.K.W. Lee, J.S. Ho, Wireless battery-free body sensor networks using near-field-enabled clothing, *Nat. Commun.* 11 (2020) 444. <https://doi.org/10.1038/s41467-020-14311-2>.
- [196] D. Hayes, F. Cappa, N.A. Le-Khac, An effective approach to mobile device management: security and privacy issues associated with mobile applications, *Digit. Bus.* 1 (2020), 100001. <https://doi.org/10.1016/j.digbus.2020.100001>.
- [197] C. A. L. J. H. W. C. H. Mobile phones in research and treatment: ethical guidelines and future directions, *JMIR Mhealth Uhealth* 3 (2015). <https://doi.org/10.2196/MHEALTH.4538>.
- [198] European Data Protection Supervisor, *Guidelines on the Protection of Personal Data in Mobile Devices Used by European Institutions*, 2015.
- [199] M. Dhingra, Legal issues in secure implementation of bring your own device (BYOD), *Procedia Comput. Sci.* 78 (2016) 179–184. <https://doi.org/10.1016/j.procs.2016.02.030>.
- [200] C. Hou, J. Zhang, J. Wang, Medical wireless IoT system and nursing intervention of chronic bronchitis based on clinical data, *Microprocess. Microsyst.* 82 (2021), 103878. <https://doi.org/10.1016/j.micpro.2021.103878>.
- [201] M. Cuquet, A. Fensel, The societal impact of big data: a research roadmap for Europe, *Technol. Soc.* 54 (2018) 74–86. <https://doi.org/10.1016/j.techsoc.2018.03.005>.
- [202] E. Anane-Sarpong, T. Wangmo, C.L. Ward, O. Sankoh, M. Tanner, B.S. Elger, You cannot collect data using your own resources and put it on open access": perspectives from Africa about public health data-sharing, *Develop. World Bioeth.* 18 (2018) 394–405. <https://doi.org/10.1111/DEWB.12159>.
- [203] M.D. Wilkinson, M. Dumontier, I.J. Aalbersberg, G. Appleton, M. Axton, A. Baak, N. Blomberg, J.-W. Boiten, L.B. da Silva Santos, P.E. Bourne, J. Bouwman, A.J. Brookes, T. Clark, M. Crosas, I. Dillo, O. Dumon, S. Edmunds, C.T. Evelo, R. Finkers, A. Gonzalez-Beltran, A.J.G. Gray, P. Groth, C. Goble, J.S. Grethe, J. Heringa, P.A.C. 't Hoen, R. Hooft, T. Kuhn, R. Kok, J. Kok, S.J. Lusher, M.E. Martone, A. Mons, A.L. Packer, B. Persson, P. Rocca-Serra, M. Roos, R. van Schaik, S.-A. Sansone, E. Schultes, T. Sengstag, T. Slater, G. Strawn, M.A. Swertz, M. Thompson, J. van der Lei, E. van Mulligen, J. Velterop, A. Waagmeester, P. Wittenburg, K. Wolstencroft, J. Zhao, B. Mons, The FAIR Guiding Principles for scientific data management and stewardship, *Sci. Data* 3 (2016), 160018. <https://doi.org/10.1038/sdata.2016.18>.
- [204] FAIR Principles - GO FAIR, (n.d.). <https://www.go-fair.org/fair-principles/> (accessed October 15, 2021).
- [205] P. Brangel, A. Sobarzo, C. Parolo, B.S. Miller, P.D. Howes, S. Gelkop, J.J. Lutwama, J.M. Dye, R.A. McKendry, L. Lobel, M.M. Stevens, A serological point-of-care test for the detection of IgG antibodies against ebola virus in human survivors, *ACS Nano* 12 (2018) 63–73. <https://doi.org/10.1021/ACS.NANO.7B07021>.
- [206] A. Priye, S.W. Bird, Y.K. Light, C.S. Ball, O.A. Negrete, R.J. Meagher, A smartphone-based diagnostic platform for rapid detection of Zika, chikungunya, and dengue viruses, *Sci. Rep.* 7 (2017) 1–7. <https://doi.org/10.1038/srep44778> (2017) 1–11.
- [207] A. Ganguli, A. Ornob, H. Yu, G.L. Damhorst, W. Chen, F. Sun, A. Bhuiya, B.T. Cunningham, R. Bashir, Hands-free smartphone-based diagnostics for simultaneous detection of Zika, Chikungunya, and Dengue at point-of-care, *Biomed. Microdevices* 19 (2017). <https://doi.org/10.1007/s10544-017-0209-9>.
- [208] A.T. Choko, P. MacPherson, E.L. Webb, B.A. Willey, H. Feasy, R. Sambakunsi, A. Mdolo, S.D. Makombe, N. Desmond, R. Hayes, H. Maheswaran, E.L. Corbett, Uptake, accuracy, safety, and linkage into care over two years of promoting annual self-testing for HIV in blantyre, Malawi: a community-based prospective study, *PLoS Med.* 12 (2015), e1001873. <https://doi.org/10.1371/JOURNAL.PMED.1001873>.
- [209] N. Gous, A.E. Fischer, N. Rhagnath, M. Phatsoane, M. Majam, S.T. Lalla-Edward, Evaluation of a mobile application to support HIV self-testing in Johannesburg, South Africa, *South. Afr. J. HIV Med.* 21 (2020). <https://doi.org/10.4102/SAJHIVMED.V21I1.1088>.
- [210] P.-Y. Chen, C.-H. Ko, C.J. Wang, C.-W. Chen, W.-H. Chiu, C. Hong, H.-M. Cheng, I.-J. Wang, The early detection of immunoglobulins via optical-based lateral flow immunoassay platform in COVID-19 pandemic, *PLoS One* 16 (2021), e0254486. <https://doi.org/10.1371/JOURNAL.PONE.0254486>.
- [211] A. Roda, S. Cavallera, F. di Nardo, D. Calabria, S. Rosati, P. Simoni, B. Colitti, C. Baggiani, M. Roda, L. Anfossi, Dual lateral flow optical/chemiluminescence immunosensors for the rapid detection of salivary and serum IgA in patients with COVID-19 disease, *Biosens. Bioelectron.* 172 (2021), 112765. <https://doi.org/10.1016/j.bios.2020.112765>.
- [212] R.M. Young, C.J. Solis, A. Barriga-Fehrman, C. Abogabir, Á.R. Thadani, M. Labarca, E. Bustamante, C.v. Tapia, A.G. Sarda, F. Sepulveda, N. Pozas, L.C. Cerpa, M.A. Lavanderos, N.M. Varela, A. Santibañez, A.M. Sandino, F. Reyes-Lopez, G. Dixon, L.A. Quiñones, Smartphone screen testing, a novel pre-diagnostic method to identify sars-cov-2 infectious individuals, *Elife* 10 (2021). <https://doi.org/10.7554/ELIFE.70333>.
- [213] S. Huang, J. Yang, S. Fong, Q. Zhao, Artificial intelligence in the diagnosis of COVID-19: challenges and perspectives, *Int. J. Biol. Sci.* 17 (2021) 1581. <https://doi.org/10.7150/IJBS.58855>.
- [214] D.A. Mendels, L. Dortet, C. Emeraud, S. Oueslati, D. Girlich, J.B.B. Ronat, S. Bernabeu, S. Bahi, G.J.H.H. Atkinson, T. Naas, Using artificial intelligence to improve COVID-19 rapid diagnostic test result interpretation, *PNAS* 118 (2021). <https://doi.org/10.1073/pnas.2019893118>.
- [215] L. Ma, L. Yin, X. Li, S. Chen, L. Peng, G. Liu, S. Ye, W. Zhang, S. Man, A smartphone-based visual biosensor for CRISPR-Cas powered SARS-CoV-2 diagnostics, *Biosens. Bioelectron.* 195 (2022), 113646. <https://doi.org/10.1016/j.bios.2021.113646>.
- [216] Ellume, Ellume COVID-19 home test - product overview for healthcare professionals. <https://www.fda.gov/medical-devices/>, 2020. (Accessed 18 October 2021).
- [217] S. Toussaert, Upping uptake of COVID contact tracing apps, *Nat. Human Behav.* 5 (2021) 2. <https://doi.org/10.1038/s41562-021-01048-1>, 5 (2021) 183–184.
- [218] M. Hatamian, S. Wairimu, N. Momen, L. Fritsch, A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps, *Empir. Software Eng.* 26 (3) (2021) 1–51. <https://doi.org/10.1007/S10664-020-09934-4>.
- [219] S. Munzert, P. Selb, A. Gohdes, L.F. Stoetzer, W. Lowe, Tracking and promoting the usage of a COVID-19 contact tracing app, *Nat. Human Behav.* 5 (2) (2021) 247–255. <https://doi.org/10.1038/s41562-020-01044-x>.
- [220] M. Zhang, A. Chow, H. Smith, COVID-19 contact-tracing apps: analysis of the readability of privacy policies, *J. Med. Internet Res.* 22 (2020). <https://doi.org/10.2196/21572>.
- [221] G. Kostka, S. Habich-Sobiegalia, In times of crisis: public perceptions toward COVID-19 contact tracing apps in China, Germany, and the United States, *New Media Soc.* (2022), 146144482210832. <https://doi.org/10.1177/14614448221083285>.
- [222] S. Rebers, N.K. Aaronson, F.E. van Leeuwen, M.K. Schmidt, Exceptions to the rule of informed consent for research with an intervention, *BMC Med. Ethics* 17 (2016) 9. <https://doi.org/10.1186/s12910-016-0092-6>.
- [223] C. Watson, J.D. Smeddinck, Unconsented data transfusions, in: *Proceedings of the Conference on Mensch Und Computer*, ACM, New York, NY, USA, 2020, pp. 205–209. <https://doi.org/10.1145/3404983.3409994>.
- [224] P. Boeing, Y. Wang, Decoding China's COVID-19 'virus exceptionalism': community-based digital contact tracing in Wuhan, *R D Manag.* 51 (2021) 339–351. <https://doi.org/10.1111/radm.12464>.
- [225] M.J. Parker, C. Fraser, L. Abeler-Dörner, D. Bonsall, Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic, *J. Med. Ethics* 46 (2020) 427–431. <https://doi.org/10.1136/medethics-2020-106314>.