Brain leaks and consumer neurotechnology

Marcello Ienca, Pim Haselager & Ezekiel J Emanuel

Greater safeguards are needed to address the personal safety, security and privacy risks arising from increasing adoption of neurotechnology in the consumer realm.

Rapid advances in neuroscience, clinical imaging, digital health and the Internet of Things are propelling neurotechnology from the exclusive domain of the medical clinic to an ever-increasing number of direct-to-consumer (DTC) applications. Today, numerous neuromodulatory devices and brain–computer interfaces (BCIs) are becoming available to consumers, with associated accessories, mobile applications, software frameworks and online services (**Fig. 1**).

DTC headsets allow individuals to engage in various activities without medical supervision, such as monitoring cognitive health and well-being, optimizing brain fitness and performance, or playing virtual games (**Table 1**). Companies such as Neurosky and Emotiv Systems offer assortments of smartphone-compatible DTC neurodevices; large electronics and social media companies, such as Samsung (Seoul) and Facebook, are testing future products controlled via electroencephalography (EEG)-detected brain signals.

As neurotechnology becomes more common outside of the clinical sphere and in the consumer market, brain derived data will increase in quantity and will require new solutions that are both capable of effective storage and sharing and that also ensure protection of privacy and security. Brain recordings in connection with other types of online information will add to the increasing proliferation of comprehensive electronic user profiles. These developments raise two fundamental questions for society and the biomedical community: Are our current digital infrastructures adequate for this upcoming proliferation of consumer-generated neurological data? And what legal and ethical safeguards need to be put in place to ensure individual rights, such as privacy and data security, are protected?

An expanding DTC universe

According to a recent review by neurotechnology market research firm SharpBrains, the number of patent classifications related to DTC neurotechnology has more than doubled in the past 10 years[1]. Currently, over 8,000 active patents are focused on neurotechnology, with just as many pending applications. Another market research analysis by *Neurotech Reports* projects an overall worldwide market for neurotechnology products of $8.4 billion in 2018 that will reach $13.3 billion in 2022. Indeed, at last year's NeuroGaming conference in San Francisco, the hyperbole rose to fever pitch, with delegates heralding the dawn of "the pervasive neurotechnology age" in which everyday wearable technologies will be noninvasively connected to brains.

DTC neuromodulatory and imaging devices open new opportunities for self-monitoring and cognitive training in fields as diverse as mental health and education. And as neurodevices increase in portability and affordability, neurotechnology is likely to become increasingly pervasive. Three types

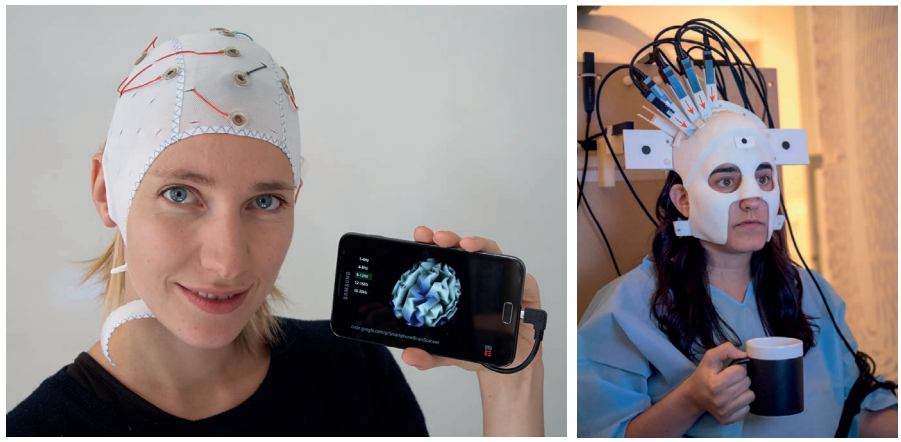

Figure 1 DTC applications of neurotechnology. (**a**) Example of smartphone-compatible and wearable EEG-based brain computer interface (BCI) for cognitive monitoring and device control[28]. (**b**) Prototype of wearable magnetoencephalography system developed by Boto *et al.*[8]. The modality in **a** is already widespread in the consumer market, whereas **b** has as yet been investigated only in the research setting. Both types of wearable system allow the recording of brain activity from subjects moving naturally and performing tasks in both natural and virtual environments. In addition, smartphone compatibility allows user-friendly, real-time monitoring and self-assessment.

Marcello Ienca is at the Health Ethics & Policy Lab, Department of Health Sciences and Technology, ETH Zurich, Zurich, Switzerland; and at the Institute for Biomedical Ethics, University of Basel, Basel, Switzerland; Pim Haselager is at the Donders Institute for Brain, Cognition and Behaviour, Radboud University, Nijmegen, the Netherlands; and Ezekiel J. Emanuel is at the Department of Medical Ethics and Health Policy, University of Pennsylvania, Philadelphia, Pennsylvania, USA. e-mail: marcello.ienca@hest.ethz.ch

Table 1 Neurotechnologies that are already marketed DTC

Device name	Manufacturer	Type of data collected	Connectivity	Price*	Advertised uses	Ethical concerns
Neuromonitoring headsets						
Muse	InteraXon (Canada)	EEG	Wireless	$249.00	Elevating meditation experience	Privacy, data security, informed consent, reliability
Insight	Emotiv Systems	EEG	Wireless	$299.00	Self-assessment, cognitive training, research, device control	
Epoc+	Emotiv Systems	EEG	Wireless	$799.00	Self-assessment, cognitive training, research, device control	
Necomimi	Neurowear (Japan)	EEG	Wireless	$49.00	Augmentation, device control	
MindWave Mobile 2	Neurosky	EEG	Wireless	$99.99	Self-assessment, meditation, gaming, device control	
Ultracortex 'Mark IV' EEG Headset	Open BCI	EEG, MEG, ECG	Wired	$499.99–599.99 (unassembled)	Self-assessment, cognitive training, research, open development	
Sleep Shepherd Blue	Sleep Shepherd	EEG (with binaural beat biofeedback)	Wireless	$199.99	Improved sleep efficiency	
Neuromodulation tools						
GoFlow	Foc.Us (US/UK)	tDCS	Wired	$139.00	Improved concentration, brain training	Safety, privacy, data security, informed consent, reliability
Focus V3	Foc.Us (US/UK)	tDCS, tRCS, tRNS, tPCS, tACS	Wireless	$399.00	Improved concentration, brain training	
Cefaly	Roxon (Canada)	External tRNS	Wireless	$349.00	Treatment and prevention of migraines	
Thync	Thync Global	tDCS, TNS	Wireless	$150.00	Improved sleep efficiency, stress release	
Fisher Wallace Stimulator	Fisher Wallace Laboratories	CES	Wired	$699.00	Treatment of depression, anxiety and insomnia	

*Price, as of May 20, 2018. CES, cranial electrotherapy stimulation; PCS, transcranial pulsed current stimulation; TNS, trigeminal nerve stimulation.

of neurotechnology that are entering the consumer products market pose the greatest concern for privacy and security: BCIs for device control or self-monitoring, devices for noninvasive neurostimulation, and neuromarketing applications of neuroimaging technology.

Self-monitoring, home therapy and neuromarketing

As yet, reports on only a few of these three different types of neurotechnology device relevant to the DTC space have been published in the peer-reviewed literature. We discuss each in turn to exemplify the types of privacy and security issues that arise when applied in the DTC market.

Self-monitoring using BCI. Portable EEG headsets, like Emotiv Epoc+ and Neurosky Mindwave, are available in the consumer market with prices ranging between $99.99 and $799.99. These products enable access to raw EEG data with a proprietary software subscription for a variety of purposes, including monitoring attention levels or controlling virtual objects. However, their privacy and security standards are questionable. In 2013, researchers used a consumer headset to demonstrate that EEG measurements of an event-related potential elicited in decision making (the 'P300') can be successfully used to extract financial and identity-related information from BCI users without their knowledge or consent[2]. In this experiment, users were exposed to various classes of visual stimuli (for example, bank cards, PIN (personal identification) numbers, area of living and the knowledge of known persons) through *ad hoc* designed 'brain spyware'; that is, software intentionally designed to extract private information from brain recordings. For each class of stimulus, one target stimulus (i.e., stimulus eliciting sensitive information known to the user) was inserted in a randomly permuted sequence of non-target stimuli. Through the analysis of the captured EEG signal, researchers were able to detect which of the presented stimuli were related to the user's private or secret information, such as the user's home address and PIN code digits. Such information leakage from the user revealed a significant chance of successful extraction of sensitive data. Compared with random guessing attacks, the EEG information can enhance identification accuracy of private information by ~15–40% on average.

Similarly, researchers at the University of Washington have developed a BCI game, called 'Flappy Whale,' in which players are presented with overt visual stimuli while EEG and magnetoencephalography (MEG) signals are recorded. The results of the experiment confirm the feasibility of extracting private and sensitive information from BCI users through subliminal stimulation. Although Flappy Whale was designed to measure responses to relatively innocuous information (for example, logotypes of commercial brands), its creators claimed during the Enigma Conference 2017 in Oakland, California, that the same model has the potential to extract more sensitive information, such as financial information or even personal beliefs[3].

Devices for noninvasive neurostimulation. Security breaches might be also enabled by another type of neurotechnology: transcranial current stimulation, which encompasses various techniques, such as tDCS (transcranial direct current stimulation), tACS (transcranial alternating current stimulation) and tRNS (transcranial random noise stimulation). Thus far, mechanisms for these approaches have yet to be completely defined: tDCS applies a

constant electric field dependent on polarity that is thought to have short-term effects on neuronal excitability, likely through cell membrane polarization; tACS applies an oscillatory electric field with a specific frequency and phase that modulates brain oscillations, supposedly through 'entrainment'; and tRNS applies white noise (1–640 Hz) to modulate cortical excitability, likely though 'stochastic resonance'. A related set of neurostimulatory devices use transcranial magnetic stimulation (TMS) to influence cortical activity.

An increasing number of the above devices are being approved by the US Food and Drug Administration (FDA) for use under prescription. But many of these neurodevices are also being marketed in the DTC realm. Commercial applications of tDCS device kits, such as Neuroelectrics' StartStim8, are of particular concern because they often rely on wireless (Bluetooth) connections between a home computer and the device, allowing unsecured data transmission that can be intercepted by third parties. For TMS, Neuronetics and eNeura have FDA-approved devices for depression and migraine, respectively; other TMS devices are also entering the consumer market. Other products are available without FDA certification.

In addition to privacy and data security issues, researchers have also questioned the safety of these neurostimulation techniques, arguing that some longer term side effects (for example, build-up of stimulating effects in non-target areas) are poorly known, and expressed concern that the adjective "non-invasive" may mislead nonexpert users into the belief that the effect of the technique is by definition mild[4]. These concerns become particularly relevant in the context of widespread and unsupervised uses of advertised DTC products, especially when some claims, such as improving cognitive performance and mental wellbeing, are not sufficiently substantiated by validated scientific evidence[5].

Neuromarketing and neuroimaging. The combination of neuroimaging techniques, such as functional magnetic resonance (fMRI), and machine learning also presents new concerns regarding breaches of mental privacy[6]. In a study conducted at the University of California, participants were shown movie trailers while undergoing an fMRI scan. Decoding fMRI data, the researchers used a machine learning algorithm to reconstruct the videos[7]. Although the reconstructed videos remained blurry, researchers effectively proved the feasibility of reconstructing content from neural data. Given the self-improving capacity of the algorithm and the increasing accuracy of neuroimaging scans, the brain-reading potential of such technology is likely to increase substantially in the near future.

In parallel, the development of innovative MEG techniques that do not require superconducting technology could lead, in the near future, to a new generation of lightweight, wearable neuroimaging headsets[8].

Although the neuroimaging tools above are not currently applied in the DTC context *sensu stricto* owing to their limited portability, the increasing application of similar devices in commercial settings opens new possibilities for collection and analysis of neural information outside the clinical or research domain. This information can be used by neuromarketing research companies to study—and possibly influence—consumer behavior and perception. Neuroimaging applications in commercial settings, especially in neuromarketing, are of particular ethical concern because they are not required to comply with the same ethical guidelines as clinical research. Unlike clinical research, neuromarketing companies are free to conduct neuroimaging studies of humans in the consumer space without formal approval from an ethics committee and rigorous informed consent from study participants. Furthermore, once DTC neuromonitoring becomes sufficiently widespread, big data analytics can be performed on large-scale datasets of user-generated neural data without explicit user consent.

Privacy and information security risks

Historically, at the early stages of technological innovation security risks are common because of a lack of stringent security measures integrated into the technologies and unprepared legal frameworks. Notoriously, "technology innovates faster than the regulatory system can adapt," and disruptive technological advancements can make current privacy and security norms obsolete[9]. For example, the frequency of cybersecurity threats has increased substantially with the disruptive emergence of smartphone-controlled pervasive and ubiquitous computing[10]. Given the high sensitivity of neural information, neurotechnology must not be allowed to follow a similar historical trajectory. Privacy and security breaches should be proactively anticipated and prevented.

The combination of three distinctive features inherent in DTC neurotechnology poses important ethical and legal challenges. First, the expansion of commercial neurodevices and neuromarketing applications produces large volumes of data (both raw EEG data and their associations with user data, demographics, social media information etc.) in an unprotected and loosely regulated manner. Second, the control of EEG data is only partially voluntary, and it may be tapped without the knowledge of the subject. Moreover, access to these raw data enables a more direct detection pathway of the neural correlates of mental processes, such as interests, intentions, silent speech, moods and preferences, compared with other digitally available sensor data[11]. And third, the data collected includes rich and personally identifiable sources of information that could be aggregated by data handlers to capture or predict elements of health status, preferences and behavior.

The comprehensive collection of both personal and nonpersonal information is common to most DTC neurotechnology actors. For example, the Emotiv Privacy Policy states that the company exercises the right to gather "personal information" from users that can be associated with them, including their EEG data, usage information, specific interactions with applications, and "information that may be inferred from the foregoing sources, either alone or in any combination" (https://id.emotivcloud.com/eoidc/privacy/privacy_policy/; accessed 8 August 2018). In addition, if Emotiv or Neurosky customers use their social network log-in to create a user profile, information associated with the social network account, such as demographics, IP (internet protocol) address and interests, will be collected and linked to the EEG data.

With the growing proliferation of neurotechnology-related online databases available for analysis and their association with digitally available profiles, it will be increasingly hard for users to selectively isolate intended information (for example, parameters relevant to cognitive self-monitoring and training) from information that they wish to keep private, such as preferences, interests or abnormalities. Anonymization techniques are useful but vulnerable to reidentification. Consequently, unintended disclosure of private information is a tangible risk[12].

Brain privacy and security risks can arise in multiple ways. First, as the brain-spyware and Floppy Whale examples show, raw neural data, such as EEG recordings, can be gleaned directly from the neuroheadset through subliminal stimulation, without authorization from the user. These activities are forms of 'brain hacking' and can exploit different phases of the BCI cycle[13].

As technology advances, the accuracy and informational richness of hacking primary brain data sources are set to increase, opening novel possibilities for unintended and unconsented decoding of mental information. In non-cybercriminal scenarios, EEG recordings and neuroimaging data collected in neuromarketing studies can be used to reveal information (for example, biomarkers of mental

illness or personal beliefs) from participants. Similarly, variations in EEG responses to Facebook interests, demographic data and other online activities could be gleaned from users of Internet-connected consumer-grade BCIs without explicit consent of the user.

What's more, data can be accessed from platforms of sensor data storage, analysis and visualization. Most DTC companies, including Emotiv, Neurosky and InteraXon, use private cloud services for data storage in which users outsource their data to an in-house or third-party cloud provider. Notoriously, cloud services are vulnerable to both insider threats and cyberattacks, especially distributed denial of service attacks. In addition, they are characterized by lack of customer support, standardization problems (absence of clear-cut guidelines unifying cloud providers), and unclear legal liability in case of security breaches. The attractiveness and therefore risk of hacking data storage sites by nefarious and criminal actors will be greatly increased when large population EEG databases are stored and linked for analysis to other databases containing medical, social-media or other sensitive information. Even though most DTC companies anonymize the collected EEG data, these data can be easily combined with other informational sources to reidentify a user. It is notable that DTC neurotechnology companies actively encourage users to outsource their data. For example, if users of most DTC services choose not to upload their data to the cloud, a more limited set of features is made available to them. Most data can also be hacked during transmission from the recording device to other platforms. This breach of security can be facilitated by unsecured uses of data gathering and sharing services. This phenomenon has already been observed in the context of mobile health, with many health professionals sharing patient-related clinical data via unsecured wireless channels like smartphone messaging apps[14]. Outside the clinical context, in the DTC sphere, the use of unsecured data-sharing services is widespread and the exposure to unauthorized access even higher[15].

The risk of unauthorized disclosure of brain information is particularly perilous among people with medical and psychological conditions. For example, the unintended disclosure of information revealing cognitive deficits and neural signatures predictive of disorders (for example, depression or bipolar disorder), substance addiction or personality traits that the person wants to keep private can lead to discrimination and social isolation[12,16].

The possibility of brain leaks is not limited to criminal hackers or other malevolent agents, and does not necessarily involve the use of malware. With the growing availability of large sets of brain-related data, anonymous EEG and fMRI data can be legally mined for commercial and marketing purposes to reveal more information about a certain user group than the individual user intended to provide or share. As long as people accept their terms of use, companies are free to use data-mining and big-data analytics to extract associations between sensor data, demographic information and online behavior or to share the data with third parties for further reuse.

Recycling of user data is a real possibility—and could become highly profitable—for private providers of DTC neurotechnology services. For example, by accepting the terms of use of most direct-to-consumer BCI providers, users grant the companies a right to reuse and disclose nonpersonal information to advertisers and other third parties. These data can be used for a variety of purposes, including identifying peer groups based on their overall cognitive performance relative to age or other characteristics. When companies like Facebook will be able to collect large volumes of brain-derived data, these policies will allow them to reuse this information for microtargeted psychographic ads or other commercial purposes.

Finally, neuromonitoring techniques are also being tested by national security agencies for surveillance, investigation and predictive policy purposes[17,18], making governments another actor potentially interested in the access and reuse of personal neurological data. This possibility projects a future in which "thoughts and images in our brains could become the target of future government investigations"[19]. To the extent the information is available in private firms, the government could, in principle, obtain access to the firms' information through search warrant, subpoena, or simple request. This is explicitly laid out in InteraXon's Privacy Policy, which states that the company may be required to share personal information to comply with applicable law or respond to governmental requests.

Inadequate safeguards

Because of the socio-technological novelty of consumer neurotechnology trends, current ethical and legal safeguards are inadequate to guarantee the protection of brain information in this rapidly changing digital environment. In the United States, federal law protects medical information. And yet, no specific laws or guidelines govern access to brain data outside of the clinical realm. If a consumer neurotechnology or associated app is provided by an hospital or business associate, then HIPAA (Health Insurance Portability and Accountability Act)[20] regulation applies. However, HIPAA does not apply if the neuroheadset is simply purchased online by an individual without a prescription and the apps are downloaded from an app store, as is usual in the DTC realm.

Consumer neurotechnology highlights the problem of regulations focusing on where the data originate rather than the nature and use of such data. In parallel, FDA regulation provides guidance for digital health and mobile medical apps[21]. However, the current FDA framework has been criticized for creating simultaneously under-regulation and over-regulation. On the one hand, it is relatively easy for DTC manufacturers to elude FDA compliance because of its limited domain. On the other hand, it is difficult for responsible innovators to invest in neurodevices that require a premarket approval path from the FDA because of the significant delays in approving new devices.

It is important to highlight that expanding HIPAA and the FDA's scope might not be possible without new legislation because those regulations can only go as far as the statutes (i.e., Congress) allow. Therefore, reforming policies for the digital health era almost certainly requires new legislation and not just agency-initiated changes in regulations.

Indeed, DTC neurotechnology applications often remain in an undefined ethical and regulatory space. For example, while neuroimaging studies in the neuroscience and clinical research setting require institutional review board approval and follow specific guidelines for data usage, consumer neurotechnology companies are not subject to the same standards. Neuromarketing companies can run studies involving human subjects without formal approval from an ethics committee. This makes it possible for DTC companies to collect substantial volumes of user-generated data and distribute them to third parties, even when the purpose of such reuse (for example, marketing analysis) could be different from the intent of the user or the function advertised by the company when selling the product (for example, self-monitoring of mental well-being)[22].

With the volume of personal neurological data rapidly increasing and security-by-design not being the focus of companies, such defective legal and regulatory coverage allows unsecure uses of brain information. As stated by Nita Farahany during the World Economic Forum in Davos, Switzerland: "There are no legal protections from having your mind involuntarily read". Not surprisingly, security experts consider BCI and other neurotechnologies to be among the nine disruptive technological trends that "are likely to shape the cybersecurity environment over the next decade"[22].

In light of these inadequate ethical and legal safeguards, the US National Institutes of Health (NIH) has recently released a request for

information, soliciting input to identify a set core of ethical issues associated with emerging neurotechnology. These include considerations associated with novel neuromodulation and neuroimaging technologies, informed consent issues in the context of neurotechnology research, and the problem of "the evolving breadth of neural data," with associated issues of data ownership, data storage and access, unintended uses of data and privacy concerns, including "protection from discrimination for those whose neural data are shared"[23]. This is helpful, but it is limited to the research setting. More importantly, the NIH has the authority to regulate research conducted with its funds, but does not have the authority to regulate the DTC market for neurodevices.

Proposing safeguards

In response to this emerging scenario, a proactive effort is needed to increase the privacy and security of brain-related data outside the medical and research context. Safeguards are needed at three levels: individual users, neurotechnology producers or service providers, and policy and regulatory bodies.

At the user level, robust and valid informed consent is critical. With the growing market of DTC self-monitoring, neurodevices and medical crowdsourcing platforms, individuals will be increasingly motivated to acquire and share their brain data as part of their quantified self, seeking interpretations of the relationship between their data and health variability—a phenomenon that has already been observed with DTC genetic testing. Given the informational richness, versatility, psychological relevance, near-endless reusability and partial voluntary control of brain data, current requests for accepting the service's terms and conditions are insufficient to protect users. In addition, the unreflective trading of one's brain data for behavior analysis or monetary compensation in neuromarketing or other services must be prevented. Research shows that most users do not fully read online terms of service[24] and hence are likely to click away their data privacy rights in an uninformed manner.

For service providers, standard practice should include the following, adopting procedures and practices similar to routine informed consent for research and stored biological samples: companies must disclose in their terms of use (1) how and where brain data are stored, (2) whether and by whom brain data are reused and shared, (3) what anonymization and information security measures are implemented, (4) how individuals will be informed if their data are hacked or inadequately transmitted, and (5) who is legally liable under those circumstances. In addition, service providers should give users the ability to easily withdraw or erase their data at any time. This would also require the incorporation into the product's license of a transparency statement of what rights and duties different parties have with respect to the data. It is necessary to replace the current click-to-accept modus for terms of service with designs that involve bullet summaries of companies' agreements and require users to explicitly consider their options.

Although companies might be granted a license to use, reproduce, display, and prepare derivative works from the user's brain-related data, they should not be automatically allowed to transmit and distribute those data to third parties. The Facebook–Cambridge Analytica scenario should not be permitted for neuro-derived information. Similarly, the linkage of sensor data with social-media profiles and other online information should be not be permitted by companies through opt-out strategies, but allowed only upon explicit affirmative permission from users via opt-in approaches. Institutional measures including an independent review board for every use of data for nonresearch purposes should also be considered. As the Cambridge Analytica scandal illustrates, online service providers like Facebook are often unwilling and unable to limit data collection, which makes it possible for third parties to access data no one gave authorization to access. This risk could be exacerbated when companies store large datasets of brain-related data.

Data security needs to be a primary concern of manufacturers and sellers of pervasive neurodevices. Proactive safeguards for the selective protection of brain-information should be incorporated into product design. One promising example is the BCI Anonymizer, a system capable of preprocessing neural signals before their transmission and storage with the purpose of removing all redundant information except the specifically intended BCI commands[25]. Distributed ledger (blockchain) computing and differential privacy techniques should also be considered as ways to improve the security and transparency of data processing. In parallel, recommendations for secured data transmission should be included by service providers in the user manual. An example of the desired standard in terms of use is Soterix Medical, which notifies users of the "risk of relying on a wireless connection with a computer to control and monitor the device." All apps—including both those bundled in the neuroheadset starter kit and those freely downloadable from an app store—should have to comply with data security best practices, such as the European Network and Information Security Agency's guidelines. In parallel, as Bonaci *et al.*[26] have observed, "platforms are immunized for apps that third parties submit," which disincentivizes manufacturers from policing abusive apps.

Finally, the often hyperbolic claims made by some DTC manufacturers need to be substantiated by more solid scientific evidence to avoid generating unrealistic expectations. Currently, companies are not required and have no incentive to wait for their products to go through expensive and time-consuming clinical or performance trials and cybersecurity tests before they market their products and make marketing claims[27]. Therefore, regulatory interventions might be required to incentivize evidence-based and user-centered development and facilitate the incorporation of efficacy, safety and security-enhancing capabilities into future prototypes.

Conclusions

In the DTC context, neurotechnology promises to improve the diagnosis and treatment of neurological disease, enable new opportunities for human-machine interaction, open possibilities for training and education, and make brain data accessible for public use. That said, cooperative, interdisciplinary efforts are urgently needed to proactively develop and implement strategies that can help maximize the benefits of pervasive neurotechnology for society at large while minimizing the privacy and security risks.

Like any other digital health subdomain, the market of consumer neurotechnology is global. Therefore, effective governance strategies should seek to harmonize national regulations. A step in the right direction is being taken in the European Union, where a new General Data Protection Regulation (GDPR) became enforceable for all member states on 25 May 2018. The GDPR requires explicit consent (opt-in) to the data collected and the purpose for which data are used "in an intelligible and easily accessible form, using clear and plain language," on pain of not being binding (Article 7.2). It obligates data controllers to meet the principles of privacy by design and by default (i.e., from the onset of the designing of systems) and to notify users in case of data breaches. Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million ($22.8 million), whichever is greater. The positive impact of GDPR on consumer neurotechnology is already visible. For example, Emotiv no longer grants itself an "irrevocable, perpetual license" to use, transmit and distribute user-generated neurological data (as was stated in their terms of use before GDPR), and the company now

informs users about their right to withdraw their consent at any time.

Creating an ecosystem that enables technological innovation while making sure that citizens have control over their data is critical for neurotechnology. All relevant stakeholders including researchers, developers, companies, regulatory agencies and end users should make security of personalized brain information a priority. Near-term solutions include enhancing the privacy and security standards of hardware and software, fostering evidence-based approaches to product development, reforming consent procedures for DTC products and raising awareness among individual users and developers. Long-term solutions include enforcing responsible governance and opening a public debate on what rights individuals are entitled to exercise in relation to their neural domain. Ignoring these issues could not only result in harm to individuals or groups but also fuel public distrust in the entire neurotechnology enterprise. Therefore, proactively securing brain-related data is the clear and present challenge to ensure continuing application of these devices in the consumer sector.

Editor's note: This article was peer-reviewed.

ACKNOWLEDGMENTS

This work was supported by the Swiss Academy of Medical Sciences (KZS 20/17).

COMPETING INTERESTS

The authors declare no competing interests.

1. Fernandez A., Sriraman, N., Gurewitz, B. & Oullier, O. Market Report on Pervasive Neurotechnology: A Groundbreaking Analysis of 10,000+ Patent Filings Transforming Medicine, Health, Entertainment and Business. (SharpBrains, San Francisco, USA, 2017). https://sharpbrains.com/pervasive-neurotechnology/.
2. Martinovic, I. *et al.* in *USENIX Security Symposium* 143–158 (2012). https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/martinovic.
3. Bonaci, T. in *USENIX Enigma* (Oakland, CA; 2017). https://www.usenix.org/conference/enigma2017
4. Davis, N.J. & van Koningsbruggen, M.G. *Front. Syst. Neurosci.* **7**, 76 (2013).
5. Medina, J. & Cason, S. *Cortex* **94**, 131–141 (2017).
6. Mecacci, G. & Haselager, P. *Sci. Eng. Ethics*, (**in press**).
7. Nishimoto, S. *et al. Curr. Biol.* **21**, 1641–1646 (2011).
8. Boto, E. *et al. Nature* **555**, 657–661 (2018).
9. Charo, R.A. *Science* **349**, 384–385 (2015).
10. Anon. Symantec. Internet security threat report. (April 21, 2016). http://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
11. Green, R.M. *Hastings Cent. Rep.* **45**, 36–37 (2015).
12. Eaton, M.L. & Illes, J. *Nat. Biotechnol.* **25**, 393–397 (2007).
13. Ienca, M. & Haselager, P. *Ethics Inf. Technol.* **18**, 117–129 (2016).
14. Mobasheri, M.H. *et al. BMJ Innov.* **1**, 174–181 (2015).
15. Sharp, R. Lacking regulation, many medical apps questionable at best. *New England Center for Investigative Reporting* **18** (2012). http://necir.org/2012/11/18/medical-apps
16. Farah, M.J. & Wolpe, P.R. *Hastings Cent. Rep.* **34**, 35–45 (2004).
17. Moreno, J.D. *Mind Wars: Brain Science and the Military in the Twenty-First Century* (Bellevue Literary Press, 2012).
18. Ienca, M., Jotterand, F. & Elger, B.S. *Neuron* **97**, 269–274 (2018).
19. Farahany, N.A. *Univ. Pa. Law Rev.* **160**, 1239–1308 (2012).
20. US Department of Health and Human Services. Summary of the HIPAA privacy rule. (Department of Health and Human Services, Washington, DC, 2003).
21. Food & Drug Administration. Mobile medical applications: guidance for industry and Food and Drug Administration staff. (Food and Drug Administration, Washington, DC, 2013).
22. Steinhubl, S.R., Muse, E.D. & Topol, E.J. *Sci. Transl. Med.* **7**, 283 (2015).
23. National Institutes of Health. NIH Request for Information (RFI): Guidance for Opportunities in Neuroethics. *NIH BRAIN Initiative* (2016) https://grants.nih.gov/grants/guide/notice-files/NOT-MH-16-014.html.
24. Obar, J.A. & Oeldorf-Hirsch, A. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. in The 44th Research Conference on Communication, Information and Internet Policy (2016). https://ssrn.com/abstract=2757465.
25. Bonaci, T., Herron, J., Matlack, C. & Chizeck, H.J. *IEEE Technology and Society Magazine* **34**, 44–51 (2015).
26. Bonaci, T., Calo, R. & Chizeck, H.J. *IEEE Technology and Society Magazine* **34**, 32–39 (2015).
27. Baker, M. *Nat. Biotechnol.* **25**, 377–379 (2007).
28. Stopczynski A, Stahlhut C, Larsen JE, Petersen MK, Hansen LK. *PLoS One* **9,** e86733 (2018).