Received: 30 June 2021 | Accepted: 14 March 2022

DOI: 10.1002/pan3.10327

PEOPLE AND NATURE | BRITISH ECOLOGICAL SOCIETY

PERSPECTIVE

Ethical ecosurveillance: Mitigating the potential impacts on humans of widespread environmental monitoring

Nathan Young[1] | Dominique G. Roche[2] | Robert J. Lennox[3] | Joseph R. Bennett[2] | Steven J. Cooke[2]

[1]University of Ottawa, Ottawa, ON, Canada

[2]Carleton University, Ottawa, ON, Canada

[3]NORCE Norwegian Research Center, Bergen, ON, Norway

Correspondence
Nathan Young
Email: nyoung@uottawa.ca

Handling Editor: Taylor H Ricketts

Abstract

1. Ecosurveillance has proliferated in recent years, generating vast amounts of data on the natural environment. Ecosurveillance also has significant potential impacts on humans; therefore, researchers and policymakers need new conceptual tools to anticipate and mitigate any negative effects.
2. Surveillance studies is an interdisciplinary field in the social sciences, providing a number of insights and practical lessons for predicting and managing the complex impacts (positive and negative, intended and unintended) of surveillance tools and practices.
3. We draw on surveillance studies literature to propose two tools to guide designers and practitioners of ecosurveillance—a 'red flag checklist' to anticipate potential problems, and a 'considerations guide' to inform design decisions across a wide range of ecosurveillance systems. These tools will help ensure that the coming era of ecosurveillance is guided by responsible and ethical practices towards wildlife and humans alike, while also realizing the potential of these technologies for improving environmental outcomes.

KEYWORDS
conservation, ecosurveillance, enforcement, ethics, social media, social power, technology

1 | INTRODUCTION

Ecosurveillance is the technology-assisted collection and analysis of data about wildlife, ecosystems, and/or people for the purposes of tracking or monitoring environmental distributions, behaviours, or indicators. Ecosurveillance is becoming increasingly important in environmental research and policy. Thousands of camera traps, continuous video streams, audio recorders, remote sensors, apps, drones, satellites and biotelemetry/biologging devices are deployed around the world to monitor territories and track the individual and group behaviour of animals and their habitats. Researchers, NGOs and government agencies (including enforcement authorities) are using Internet and social media surveillance tools to identify and monitor species distributions and behaviour, document pro- and anti-environmental human activities and identify trends in how people experience and talk about nature. Ecosurveillance therefore has tremendous upside for environmental protection and conservation, allowing researchers and authorities access to critical data to enhance scientific understanding, enforce regulations and improve decision-making. Most of the literature on ecosurveillance is consequently optimistic and celebratory in tone, as new methods, technologies

and applications rapidly emerge (e.g. Hussey et al., 2015; Jarić et al., 2020; Trouille et al., 2019).

However, pervasive and underregulated ecosurveillance also has risks and downsides, and a literature is now emerging to identify potential problems and suggest solutions. For instance, a number of recent articles address the threat posed by tracking and location data to endangered or overexploited species, and propose new data protection protocols to mitigate these risks (e.g. Tulloch et al., 2019; Chapman, 2020; Lennox et al., 2020). The conversation about potential impacts on humans is different, however. Human rights and interests are complex, and people have cultural and legal expectations of privacy, equity and justice that do not apply to wildlife and environments. A small but growing number of articles address potential impacts of ecosurveillance on people, including invasions of privacy, harvesting data and information without consent, and high potential for discrimination against vulnerable and minority groups (e.g. Arts et al., 2015; Di Minin et al., 2021; Sandbrook et al., 2018; Sandbrook et al., 2021).

The antidote to many of these problems is to promote responsible and informed design of ecosurveillance projects and systems (Lennox et al., 2020). In this Perspective article, we propose two conceptual tools to help researchers and policymakers anticipate and mitigate potential negative impacts of ecosurveillance on people. These tools—a red flags checklist and a considerations guide—are intended to encourage responsible front-end design of environmental monitoring and surveillance systems. We designed these tools based on two sources: (1) the nascent literature on the potential negative impacts of ecosurveillance on people (e.g. Sandbrook et al., 2021), and (2) insights about the link between surveillance and social power from the more established social science field of 'surveillance studies' (e.g. Ball et al., 2012). We stress that we do not conduct systematic reviews of these two literatures or subject them to content coding. Given that this is a Perspective article that presents our collective views on an emerging topic, we conduct a more limited 'integrative review' of major works in the two literatures guided by our group's prior knowledge and research experience, with the aim of 'assessing, critiquing, and synthesizing the literature on a research topic in a way that enables new theoretical frameworks and perspectives to emerge' (Snyder, 2019: 335). Combining insights from these two literatures, we provide practical and comprehensive advice for ecosurveillance practitioners working with an ever-growing array of data-gathering technologies.

2 | TYPES AND TECHNOLOGIES OF ECOSURVEILLANCE

Ecosurveillance is a useful umbrella term for a range of research, activist and governance activities that use monitoring technologies to generate large amounts of data for environmental and conservation purposes. Some examples of ecosurveillance goals and technologies are provided in Table 1. Ecosurveillance activities are conducted by many actors, including scientists, governments, companies, NGOs, Indigenous communities, hobbyist clubs and private individuals (Cooke et al., 2017). The goals of ecosurveillance vary, and include scientific inquiry, compliance and enforcement, monitoring habitat destruction or recovery, protecting Indigenous rights, detecting the arrival of invasive species or disease and satisfying legal and regulatory obligations for environmental assessments and monitoring (Thompson et al., 2020).

Every ecosurveillance initiative is unique in its methods and context, and presents practitioners with different ethical challenges and considerations. As a starting point, it is important to distinguish between ecosurveillance that targets humans and human activities directly, and ecosurveillance that focuses more on wildlife and/or environments. Direct targeting of humans is often associated with compliance, protection and enforcement goals (Sandbrook et al., 2021). These include measures to investigate and apprehend poachers or wildlife traders, monitor illegal logging, fishing, or mining, track tourists entering sensitive areas and report compliance with emissions or pollution regulations. For example, researchers in Costa Rica were recently able to track poaching and illegal wildlife market activities using false sea turtle eggs implanted with GPS trackers (Wetzel, 2020). Ecosurveillance can also be preventative, intervening to discourage or pre-empt illegal activities. For example, advances in drone technology make these tools attractive for monitoring animal populations and geographic areas vulnerable to exploitation (Radjawali & Pye, 2017; Wich & Koh, 2018). Video surveillance coupled with facial recognition technology is being deployed in some parks and conservation zones to alert staff to potential poaching incidents before they occur (Borno, 2019).

Other forms of ecosurveillance focus more on wildlife and environments. Research on animal populations and behaviour can be done using biotelemetry, aerial observation, thermal imaging and remote sensing equipment such as camera traps and audio recorders. The presence and prevalence of organisms can be identified using environmental DNA (eDNA) sampling. Environmental quality monitoring, including of air and water chemistry, increasingly makes use of Internet enabled remote sensing to provide continuous readings (Abraham et al., 2017). This type of ecosurveillance often still involves people, however. A number of the examples in Table 1 use people to generate data on wildlife and environments. For example, citizen science initiatives such as e-Bird (ebird.org) and iNaturalist (inaturalist.org) are growing rapidly, inviting participants to geotag sightings, enter observations and upload video and audio to online databases (e.g. Trouille et al., 2019). Partnerships between researchers and Indigenous communities to conduct environmental monitoring are also becoming more common (Thompson et al., 2020). iEcology and culturomics are two other emerging techniques for gathering information on wildlife and environments, by web crawling and 'scraping' large amounts of photographs, video and text data posted to social media sites for continuous analysis by artificial intelligence (AI) software (August et al., 2020; Jarić et al., 2020). Unlike citizen science, iEcology and culturomics do not involve participants volunteering information, but gather and analyse data from across the public

TABLE 1 Examples of ecosurveillance

Purpose	Select examples
Direct surveillance of humans or human activities	
Criminal investigation and conviction	Use of geolocation technology for investigation of poachers, wildlife traffickers and illegal markets
Monitoring of potential illegal behaviour	Use of camera and data surveillance to monitor spaces and/or species of concern from illegal harvest or incursion; use of facial recognition to identify people; culturomics to identify themes in online messaging; collaborative databases to report unauthorized forestry, fishing, mining and pollution events
Protection of indigenous rights	Documenting activities and harvest levels in traditionally used territories
Direct surveillance of wildlife or environments (with indirect surveillance of humans)	
Wildlife population monitoring	Citizen-science reporting of sightings or interactions; field counting; use of remote sensing on wildlife corridors; animal biotelemetry; eDNA to assess presence/absence; thermal imaging; iEcology to identify wildlife in social media images and video
Animal behaviour monitoring	Use of animal biotelemetry, camera traps and audio recording to capture animal behaviour in the wild
Environmental quality monitoring	Use of remote sensing and measurements by citizen scientists to assess and air, water and soil quality/pollution
Detecting and tracking diseases	Use of citizen science, AI, eDNA, genomics and iEcology to detect disease/disease vectors and monitor spread
Detecting and tracking biological invasions	Use of eDNA, biotelemetry, citizen science and iEcology to identify and monitor presence of invasive species
Monitoring of habitat	Use of Google Earth, remote sensing, aerial photographs (drones, aircraft, satellite) to look for changes in land and waterscapes

Sources: Blumstein et al. (2011); Hussey et al. (2015); Mohanty et al. (2016); Kays et al. (2019); August et al. (2020); Jarić et al. (2020); Thompson et al. (2020).

Internet without people's knowledge. These techniques have been used for a range of purposes, including tracking the illegal wildlife trade, monitoring invasive species, observing rarely seen hunting and predation events, and estimating population numbers (e.g. Daume, 2016; Di Minin et al., 2019; Maritz & Maritz, 2020). Finally, we note that ecosurveillance has emancipatory potential for some marginalized populations who are able to mobilize and control deployment of these tools and technologies. For example, a number of case studies have shown how Indigenous communities are using ecosurveillance to document resource usage and conservation, and to engage in 'countermapping' projects that push back against discriminatory government policies and restrictions on Indigenous rights (e.g. Radjawali & Pye, 2017; Thompson et al., 2020).

3 | INSIGHTS ABOUT HUMAN IMPACTS FROM THE LITERATURE ON ECOSURVEILLANCE: RAISING AWARENESS OF POTENTIAL PROBLEMS

The rapid expansion of ecosurveillance technologies and systems is outpacing our understanding of their impacts, particularly on people. Few articles deal directly with the impacts of ecosurveillance on humans, but the small existing literature contains highly valuable insights. As a guiding principle, Sandbrook et al. (2018) argue that collecting data about animals and environments also involves collecting data about people, even if indirectly and unevenly. This is because environments surveilled using remote sensing are also occupied, frequented and used by people. Animals tracked using telemetry interact with hunters and fishers, camera traps are triggered by people walking in wild areas, acoustic devices pick up human conversations, eDNA surveys collect human samples, automated analysis of social media collect information about individuals in photos and videos, and large databases are built by citizen-scientist contributors who voluntarily provide information about their encounters with nature. This core insight means that all forms of ecosurveillance, not just those that directly target people, should be looked at through a lens of impacts on humans.

With respect to case studies, the most extensive discussions in the current literature on human impacts deal with visual surveillance technologies, such as drones and camera traps. Sandbrook (2015) discusses the potential for drones to invade privacy and instill feelings of fear among those who encounter them in nature. Butler and Meek (2013) provide a legal analysis of potential privacy violations from camera traps in the case of Australia. Sandbrook et al. (2018) surveyed researchers who use camera traps, and found high levels of 'human bycatch' from these technologies, as well as uncertainty among researchers on how to deal with these data. Sharma et al. (2020) propose a code of conduct for camera trap users to balance privacy concerns with the obligation to report photographic capture of illegal activities.

This is also a concern for Wearn et al. (2019), who warn against the indiscriminate use of AI to analyse photo and video evidence of human behaviours, cautioning it could easily mistake the actions of innocent people for those of poachers.

Discussions are also beginning among researchers involved in citizen science about the ethics of data stewardship, commercial exploitation and privacy protections for contributors (e.g. Ceccaroni et al., 2019; Resnik et al., 2015). Researchers are similarly developing methods to anonymize scraped Internet and social media imagery, labels and text that contain or refer to people (Di Minin et al., 2021). More broadly, Sandbrook et al. (2021) present a set of 'principles for the socially responsible use of conservation monitoring and data' that apply to a range of technologies that 'accidentally or deliberately collect data on humans'. They use the term conservation surveillance technologies (CSTs), that include cameras, drones, citizen science apps and social media scraping. They identify a number of ethical concerns with data collection on humans, and advance a 'process flowchart' with high-level self-interrogation questions for researchers using CSTs. Considered together, this literature has helped to raise awareness of these issues, and provides a valuable head start in conceptualizing potential ethical problems and dilemmas with ecosurveillance.

4 | INSIGHTS FROM SURVEILLANCE STUDIES: SURVEILLANCE AS SOCIAL POWER THAT REQUIRES MITIGATION

In this Perspective article, we advance scholarship on ecosurveillance by incorporating and applying insights from the theory-rich field of surveillance studies in the social sciences. Surveillance studies is a multi-disciplinary field of study with contributions from sociology, political science, psychology, law and information studies (e.g. Lyon, 2001). It represents a coordinated attempt to conceptualize and empirically investigate the role and impact of pervasive surveillance on individuals, groups and whole societies (Ball et al., 2012). Surveillance has been a major topic of inquiry in the social sciences since the pioneering work of Michel Foucault in the 1970s on panopticon or 'all seeing' technologies and governance systems (Foucault, 1975). Foucault's key insight was that surveillance is an exercise in power that causes deep changes in human behaviour at the individual and collective levels. Being watched, or even the idea of being watched, causes individuals and groups to self-discipline without active coercion.

A theoretical cornerstone of surveillance studies inherited directly from Foucault is the assertion that surveillance is a form of social power that requires stringent regulation and ethics guidance to mitigate impacts and avoid abuse (Lyon, 2010). Sometimes imbalances of power between watcher(s) and watched are dramatic and obvious, such as when government authorities investigate crimes or monitor behaviours for lawful compliance (Brayne, 2020). In other cases, the imbalances of power are subtle but still present and highly consequential. For example, surveillance is increasingly carried out by non-governmental actors, such as private companies, consultants, communities and researchers. These actors are rarely intentionally oppressive, but they exercise power by gathering information and influencing the freedoms and behaviours of others in both direct and indirect ways (Zuboff, 2019). Acknowledging and interrogating the link between surveillance and social power allows us to think more constructively about how to manage power relations in ecosurveillance and respond pro-actively with better system design.

Table 2 presents insights from conceptual thinking and empirical research in surveillance studies in summary form, with special attention to issues of power. Some insights relate to the types and impacts of surveillance. Others come from studies of policy and regulation, and still more from research into issues of privacy and consent. For reasons of space, we discuss only a selection of these insights in the main text.

Starting with the section on types and impacts of surveillance, one of the most important insights is that surveillance can have positive and negative outcomes, often simultaneously. Much of this depends on context and the design of surveillance systems (Marx, 2015). Surveillance to enhance a public good (e.g. health monitoring, crime prevention and environmental integrity) is generally seen as legitimate and beneficial, but this easily tips into negative social perceptions and impacts if surveillance power is abused, for instance if surveillance is intrusive or if data are used for other ends that are less acceptable, such as genetic data collection or third-party marketing. Protocols for appropriate and beneficial data collection, sharing and analysis must be contextual and ethically defensible (Marx, 1998).

Some research also makes a distinction between detailed data collection and trace data collection (e.g., Thylstrup, 2019). Trace data are partial and incomplete, and therefore, involve a significant degree of uncertainty. For example, recording an IP address does not indicate who exactly is using a computer. When someone enters a store with video surveillance, their faces and bodies are recorded but their identities are not immediately discernable. However, in both cases identity might be revealed in combination with other data, such as browser logins, credit card transactions or facial recognition technology. Yet, this additional information is not always necessary for consequences to be felt. For instance, when a photoradar installation captures a speeding vehicle, there is uncertainty about who is driving, but it is the registered owner who receives the fine nevertheless. Assumptions based on trace data are therefore both powerful and difficult for the surveilled to contest or correct. Trace data have particular implications for ecosurveillance. Much ecosurveillance is over animals and environments, but collects trace data about humans who interact with them. Trace data can come from many sources, including user-contributed geolocation of sightings, inadvertent photographic, video and audio capture, data about harvesting levels, locations and behaviours, and fragments of human DNA. Trace data collection in ecosurveillance poses a number of ethical challenges that we discuss below, including difficulties acquiring consent and high potential for misidentification.

TABLE 2 Key conceptual insights and empirical lessons from surveillance studies

Theme	Insight/lesson
Types and Impacts	Surveillance can have positive and negative outcomes, often simultaneously[a,b,m]
	Surveillance today is more about the generation, storing, and analysis of data than it is about visual 'watching'[b,c]
	Surveilling events and environments also means surveilling people, even if indirectly and/or through 'traces'[d,e]
	Surveillance is increasingly conducted by private organizations and networks; data generated by surveillance are highly commercially valuable and becoming more so[c]
	Surveillance is increasingly 'participatory', involving data voluntarily provided by individuals or groups[c]
	Covert and overt surveillance have different goals and impacts on people; most data-based surveillance is overt but opaque (i.e. people know they are being surveilled but are not aware of all potential sharing and uses of the data)[c,f]
	Overt surveillance has a chilling effect on human behaviours, including legal and legitimate behaviours[b,g]
	Surveillance technologies and systems can be unintentionally discriminatory[h,l,l,n]
Policy	Policy lags technology and practice; most regulations are reactive and arise in response to public pressure[i,j]
	Most policy aims to regulate the sharing and use of data, while data collection is poorly regulated[i]
	Surveillance practices are more regulated in the public sector than in the private sector[j]
	Most surveillance policy is rights-based, rather than restrictive of technology; it is more concerned with protecting the rights of the surveilled rather than regulating technology directly[i,j]
	Most surveillance policy is sectoral and limited. This means that surveillance assemblages, which involve multiple institutions sharing data, are poorly regulated[k]
Privacy	Expectations of privacy differ in different environments and spheres of public and private life[g,j]
	Privacy is both an individual and a societal phenomenon; erosion of individual privacy can have impacts on society[b,h,m]
	Privacy can refer to exclusion (the right not to be surveilled), anonymity (identity is not knowable), and confidentiality (data are not shared and/or identity is not revealed); each dimension raises different ethical questions[g]
Consent	Surveillance should be as narrow-scope as possible, with a clear and justifiable purpose (it should be both proportionate and necessary); it should not be open-ended or indeterminate[a,g,m]
	Consent for the collection and use of data should be sought and secured[a,b,c]
	Surveillance for law-enforcement purposes should be subject to judicial oversight[g,j]
	For non-enforcement surveillance, surveilled people should have the opportunity to review, correct, and retract data about themselves[a,b,h,m]

Sources: Marx (2015)[a]; Lyon (2001)[b]; Zuboff (2019)[c]; Andrejevic and Gates (2014)[d]; Thylstrup (2019)[e]; Brayne (2020)[f]; Macnish (2017)[g]; Ball et al. (2012)[h]; Bennett (2012)[i]; Rule (2012)[j]; Haggerty and Ericson (2000)[k]; Monahan (2017)[l]; Marx (1998)[m]; Dubrofsky and Magnet (2015)[n].

Surveillance studies research also tells us that the visibility of surveillance systems has a substantial impact on human behaviours. Covert surveillance is hidden and is meant to monitor people engaged in naturalistic behaviour (as with classic investigatory surveillance). Overt surveillance however is meant to be visible, such as cameras in public spaces, to encourage and discourage certain behaviours before they happen. Overt surveillance might reduce criminal behaviour, but it is also known to have 'chilling effects' that discourage people from engaging in legal and legitimate behaviours (Manokha, 2018). In the ecosurveillance context, chilling effects might apply to legitimate licensed activities such as hunting and fishing, or even more casual activities such as hiking, camping or boating in surveilled environments.

Another important insight about social power is that surveillance has discriminatory tendencies, both intentional and unintentional. Religious and ethnic minorities are often intentionally targeted by surveillance on national security grounds (Selod, 2018). Unintentional discrimination is a more subtle problem, woven into the design of surveillance systems in a manner akin to problems of systemic racism. For example, monitoring of high crime areas or public outdoor spaces are far more likely to result in surveillance of the poor and marginalized, many of whom are forced into public spaces due to homelessness or exclusion from indoor gathering places (Monahan, 2017). With respect to ecosurveillance, monitoring of a particular territory will generate data, directly or indirectly, about the behaviours of people who occupy or frequent those spaces. Marginalized groups tend to live in polluted or contaminated spaces that might be subject to environmental monitoring (Banzhaf et al., 2019). Indigenous people's legitimate traditional, subsistence or small-economy activities might be subject to added scrutiny because they occur in spaces, or with particular species, targeted by ecosurveillance conducted by researchers and government agencies.

With respect to policy, surveillance studies research tells us that law and regulation of surveillance practices lag technological innovations by a significant margin, with governments often dragging their feet until compelled by public pressure to act (Bennett, 2012). Privacy law and policy vary significantly across the globe. However, in democracies, public sector organizations (e.g. government agencies, public service providers and public universities) are generally more constrained by regulations than private companies (Solove, 2004). Additionally, the literature tells us that most policies treat surveillance as a segmented activity that generates separate pools of data (for example, a person generates credit card data, Facebook data and public transit use data that are considered distinct). This neglects the increasing influence of 'surveillance assemblages' (Haggerty & Ericson, 2000), which involve multiple organizations selling or sharing data continuously with one another, such as policing agencies providing crime data to insurers. This cross-sectoral integration multiplies the social power of surveillors and is likely to continue with technological advancements. It potentially applies to many forms of ecosurveillance data, particularly those that involve large collaborative datasets from multiple sources.

Surveillance studies scholarship provides important insights about privacy and consent. The literature sees privacy as an imprecise umbrella term for a range of moral standards that vary across individuals, circumstances and societies (Solove, 2004). Rule (2012) helpfully encourages us to think about privacy both as an individual and a public good. For individuals, expectations of privacy may be highly contextual and subjective, but we can still speak about the erosion of privacy at the societal scale as having broad sociological impacts on norms and freedoms. As such, it is argued that surveillance should be as narrow-scope as possible, with a clear justifiable purpose (Macnish, 2017).

Consent is an important means of mitigating power imbalances. There are circumstances in which consent is impractical or undesirable, such as law enforcement operations (for which proper judicial oversight should substitute). In non-enforcement circumstances, meaningful and informed consent of the surveilled should be secured whenever possible, and surveilled people should have the opportunity to review, correct and retract data collected about themselves (Macnish, 2017; Marx, 1998). We note, however, that poorly or insidiously designed mechanisms for acquiring consent can also be a means of coercion. For example, many surveillance systems offer people an option to 'opt out' that also involves a denial of service (Marx, 1998). Surveillance studies scholars point out that many apps and software licences require consent for data collection as a condition of use, or else make opting out so cumbersome that most users accept terms for data collection and use without understanding them (Zuboff, 2019). In the ecosurveillance context, opting out can involve denials of entry to specific places (surveilled parks and amenities), access to environmental information, or participation in activities such as hunting and fishing. Care must be taken to make refusal of consent a meaningful, realistic and low-cost option to individuals and groups who do not wish to be surveilled.

5 | A RED FLAG CHECKLIST FOR ECOSURVEILLORS

Proper design and management of ecosurveillance can enhance its benefits while mitigating power imbalances and potential negative impacts on people. In this section, we propose a 'red flag' self-assessment checklist tool for researchers, policymakers and practitioners of ecosurveillance to help identify potential issues with specific plans and projects (Table 3). The red flag checklist is intended as a quick signalling tool to respond to some key issues raised in the two literatures discussed previously.

The first red flag concerns the potential for misidentification or false positives. False positives occur when people are misidentified as perpetrators or risks, and can have serious personal consequences including long-term stigmatization (Macnish, 2017). With respect to ecosurveillance, efforts to track poachers or shame trophy hunters (for instance, by analysing social media photographs and video) has high risk of false positives. So too does the use of AI or algorithms for facial recognition or behaviour analysis, particularly 'predictive AI' that

TABLE 3 Self-assessment checklist for potential red flags for ecosurveillance activities

Potential issue/red flag	Indicators/scenarios/examples	Mitigations
High potential for misidentification or false positives	Law enforcement or regulatory surveillance; large number of innocent bystanders; reliance on AI, algorithms and/or assumptions from trace data	Extreme caution in data interpretation; data and identity verification prior to intervention; caution in using AI analytics and decisions
Difficulty/inability to ensure anonymity or confidentiality	Data collection from multiple sources; combining or merging of databases; inadvertent collection of identifying information; possibility of subpoena	Clear and understandable guidelines for user-generated content and communities; continuous monitoring and revision of databases
High potential for discrimination	Profiling particular groups as eco-risks; surveillance of a territory, species, or activity primarily frequented or used by an identifiable group (e.g. an Indigenous group or community)	Very high moral and necessity bar for intentional discrimination; high levels of awareness and vigilance to anticipate and minimize unintentional discrimination
High level of vulnerability among the surveilled	Surveillance (direct or indirect) of people with low social or political power, and/or of populations whose subsistence or livelihood may be impacted by data collection or findings	Co-production of ecosurveillance research; allowing vulnerable groups to participate in decisions about design, analysis, and use of data; seeking informed prior consent
Difficulty/inability to acquire consent from and/or to inform the surveilled	Large-scale or geographically dispersed data collection; data collection in highly frequented places; unclear stakeholders or constituencies	Proactive efforts to acquire consent and to inform; allowances for the surveilled to opt-out/remove data whenever possible without repercussions or denial of service
High potential for chilling effects on legal and legitimate activities	Data collection related to controversial but legitimate activities (e.g. angling or hunting for charismatic species)	Transparency about the collection, analysis, and use of data; clarity about protocols for data sharing or secondary use; proactive communications plan
Difficulty/inability to protect data (preventing copying, hacks or sharing) or to limit secondary use by other organizations and/or participants in data collection	Collaborative research or monitoring projects; collaboratively populated databases (e.g. citizen science); cloud computing	Efforts to protect data using passwords and/or two-factor identifications; clear data access and data-management protocols; agreements about acceptable secondary use of data

is meant to anticipate human behaviours (Brayne, 2020). Trace data collection on humans can also lead to false positives if incorrect assumptions are made. For example, geographic patterns in animal death may be due to human activities (e.g. luring and trapping) or unknown natural causes. We recommend extreme caution in data interpretation and reliance on AI for enforcement decisions to mitigate this concern.

Second, a difficulty or inability to ensure anonymity or confidentiality is a red flag. This is a notable concern for citizen-science or user generated data, which increasingly offers options for uploading photographs, audio and video. Tagging places, people and events in such content is increasingly prevalent and difficult to police, as is sharing information across platforms (i.e., simultaneous posting to eBird and Facebook or Twitter). Such practices pre-empt possibilities for anonymity and confidentiality. They should be mitigated by careful drafting of codes of conduct for citizen-science and continuous review and secure curation of user-generated databases (Di Minin et al., 2021; Resnik et al., 2015).

A third red flag is high potential for discrimination. As discussed earlier, surveillance systems can be both intentionally and unintentionally discriminatory, including ecosurveillance. With respect to intentional discrimination, researchers and policymakers should ask: is any group being singled out for surveillance, particularly for law enforcement or compliance reasons? If yes, is this discrimination necessary and morally justifiable (e.g. to prevent imminent and irreparable environmental harm)? Unintentional discrimination raises different questions. It can occur when ecosurveillance is conducted on a territory, activity or species that is occupied, frequented or harvested by particular people. Researchers and policymakers should ask themselves whether ecosurveillance systems could lead to any undue scrutiny of particular groups, and/or any immediate or future threat to traditional, cultural, and subsistence activities? We believe that Indigenous people and minority groups living in stressed or polluted environments are particularly vulnerable to such effects. We also recognize that women are particularly vulnerable to power imbalances and negative impacts from surveillance (Dubrofsky & Magnet, 2015), and that women's participation in subsistence and foraging activities in some societies place them at high risk of oversurveillance and discrimination (Sharma et al., 2020). We recommend a high level of attentiveness to these challenges, and direct engagement with marginalized communities who may be affected by ecosurveillance projects, as a primary mitigation measure.

Connected to this but also distinct, a fourth red flag is a high level of vulnerability among the surveilled. Some people might be inconvenienced by the collection of detailed or trace data about their activities (for example, recreationalists), while others may have their livelihoods or subsistence directly threatened. We recommend that vulnerable groups be invited to participate whenever possible in project design and data analysis following the coproduction model

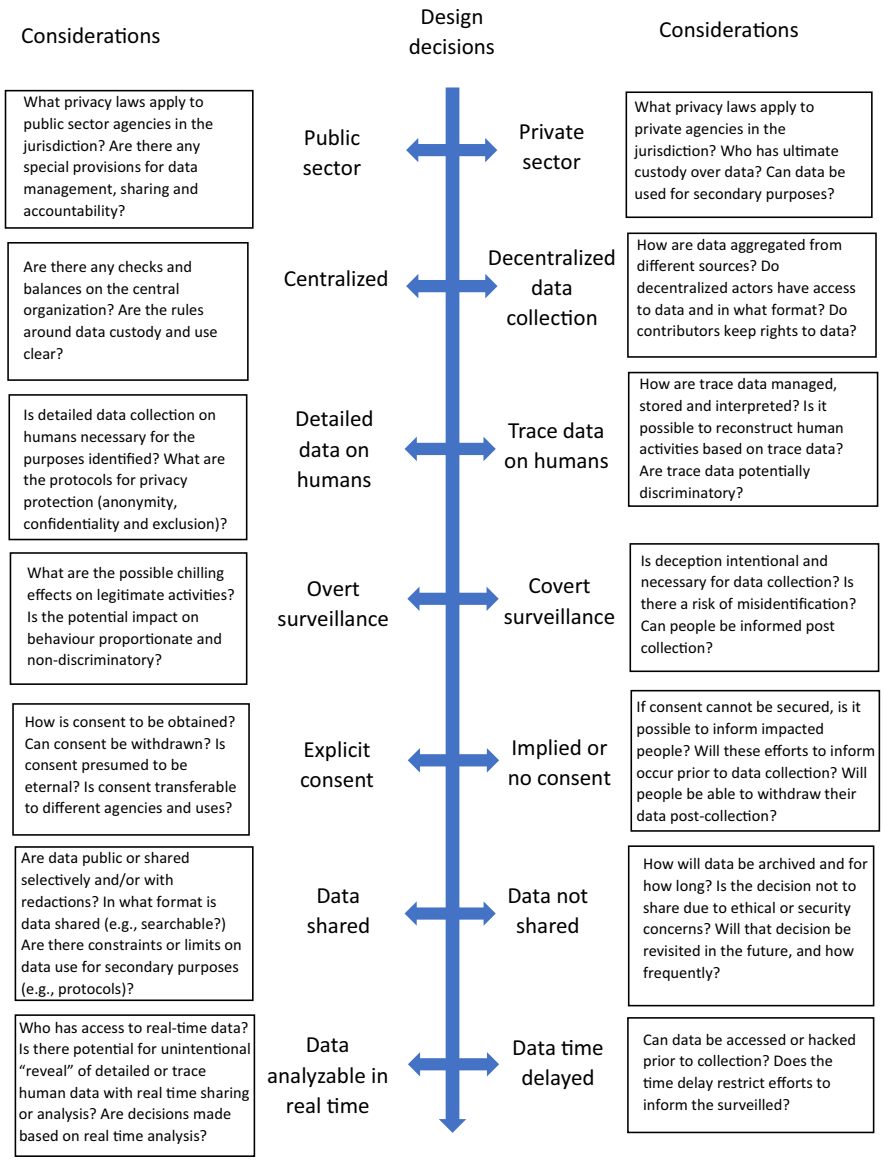

FIGURE 1 A considerations guide for ecosurveillance practitioners

(Cooke et al., 2020). This would allow such groups to steer design decisions, provide consent for data collection and extend a measure of control over data use and potential impacts.

A fifth red flag involves difficulty acquiring consent or, less ideally, informing surveilled people about data collection (this flag evidently does not apply for justifiable covert surveillance for enforcement purposes). Informing the surveilled and acquiring consent are often challenging with ecosurveillance, meaning that this red flag is frequently raised (Sandbrook et al., 2021). These challenges are most acute when ecosurveillance is conducted at a large scale or over large geographic areas, when only trace data are collected on human activities, when spaces are highly frequented (in parks or urban environments), when data collection is decentralized (as with citizen science) and when it is unclear who are the stakeholders or constituencies to inform or from whom to seek consent. We recommend that communications and consent efforts be rigorously planned and conducted as early as possible in the project design process. Options to opt-out pre-collection or remove data post-collection should be available if possible, but are admittedly difficult to implement for trace data. In cases where consent can be requested, it is important that its withholding not result in unreasonable repercussions, such as denial of service (e.g. access to licences, entry into parks, or continued use of hobbyist apps).

Sixth, ecosurveillance with high potential for chilling effects on legitimate activities should raise a red flag. This is most likely to occur with data collection related to controversial activities, such as angling for certain species or hunting for charismatic animals. Chilling effects are normative, meaning people adjust their behaviours based on an aversion to being perceived in a negative moral light (Stoycheff et al., 2019). The best antidote to chilling effects is therefore high levels of trust in the collectors and custodians of data (Macnish, 2017: 34). Trust is built over time through communication and transparency about the purpose of tracking and monitoring, as well as controls over use of the data.

The final red flag on our checklist is a difficulty or inability to protect data from copying, hacks, or sharing and/or from unforeseen

secondary uses by other organizations or individuals. These risks are particularly acute in collaborative projects that reach across sectors (academic, government, private sector), as well as in citizen-science or user-generated data initiatives (Lennox et al., 2020). Projects involving multiple organizations are susceptible to having data appropriated by broader surveillance assemblages (Haggerty & Ericson, 2000), while much citizen-science and user-generated data are never fully controlled by one entity (Resnik et al., 2015). Immediate data security concerns can be addressed using known means, such as restricted access to raw data and two-factor identification for authorized persons. Secondary use concerns are more challenging because they can extend well into the future. We recommend that practitioners of ecosurveillance develop clear protocols for data access, sunset clauses on partnerships that involve data custody agreements, clear plans for the archiving or deletion of data and negotiated expectations about acceptable secondary use of data.

6 | A CONSIDERATIONS GUIDE FOR DESIGNING ETHICAL ECOSURVEILLANCE SYSTEMS

In this section, we unite the previous discussions of ecosurveillance types, lessons from the ecosurveillance and surveillance studies literatures and identification of potential red flags to propose a 'considerations guide' for key design decisions of ecosurveillance systems and practices. The guide is presented in Figure 1. The directional arrows refer to design or practice decisions, for instance whether the system will involve centralized or decentralized data collection. Of course, it is possible that a system will involve both options, in which case both sets of considerations will be relevant. The same applies for each dimension in Figure 1 (public sector or private sector involvement, collection of detailed or trace data on humans, overt or covert surveillance approaches, etc.). We encourage researchers and regulators making decisions about ecosurveillance design to trace their preferences down and across the directional arrows in the figure. We have presented the considerations associated with each dimension in the form of questions. Some of these questions are food for thought (e.g. 'what are the possible chilling effects of surveillance?'), others are intended to elicit concrete answers (e.g. 'how will data be archived and for how long?'). The advantage of posing questions is that they apply broadly to different types and forms of ecosurveillance (as considerations rather than prescriptive guidelines). We offer them as signposts for further reflection and planning to make ecosurveillance responsive to the potential ethical challenges and dilemmas identified above.

7 | CONCLUSION

Technological innovations and accelerating environmental problems are driving ecosurveillance forward, both as a means of conducting research and as a tool for activism, policymaking and management. It is important to conceptualize ecosurveillance as a diverse but distinct form of surveillance that involves the intersectional tracking and monitoring of wildlife, ecosystems and people. Ecosurveillance has tremendous upside for scientific inquiry, evidence-based decision-making, investigating and preventing environmental crimes, and (in some cases) empowering marginalized communities. However, ecosurveillance also poses significant ethical problems and dilemmas. Some of these are about the exploitation of animals and protection of environments, and tools are being proposed in the conservation literature (e.g. Chapman, 2020; Lennox et al., 2020; Tulloch et al., 2019). Other ethical problems and dilemmas involve humans and work to understand and address these is only beginning (Sandbrook et al., 2021). We have used the nascent literature on the human impacts of ecosurveillance, alongside insights from surveillance studies about the connections between surveillance and social power, to discuss the applicability of key concepts such as false positives, chilling effects, intentional and unintentional discrimination, secondary use, surveillance assemblages, denials of service, privacy protections and the importance of consent.

The red flags checklist and considerations guide are meant to ground these considerations in real world scenarios and decisions facing researchers and policymakers who presently engage in ecosurveillance or may do so in the future. There is much more work to be done. Ecosurveillance as a concept requires further development and research, as the intersection of animal, environmental and human surveillance is poorly understood. More case research using interviews, focus groups and surveys needs to be conducted that investigates people's perceptions of ecosurveillance and trade-offs between the costs and benefits of its use. The applicability of potential mitigation strategies also needs to be investigated, particularly whether co-production, enhanced data security measures, rules for user-generated data and citizen-science, rights to see and amend personal data and secondary use of data protocols can mitigate ethical problems.

Truly addressing power imbalances in ecosurveillance over the long term likely requires more radical thinking about control over technology and data. Surveillance is typically conducted by powerful actors, and the act of surveilling extends their power by generating valuable data and by influencing the behaviours of the surveilled (Ball et al., 2012). To fundamentally shift these power dynamics, marginalized communities must be provided financial and technical resources to design, conduct and analyse their own ecosurveillance projects. For example, scientists and government authorities must commit to supporting indigenous monitoring and to allow communities to retain control over data collected. Giving up surveillance power may be difficult for traditionally privileged actors, but this is essential for ensuring that ecosurveillance technologies are deployed ethically and equitably over the long term, and that they broad support and legitimacy with the general public and directly affected communities.

ACKNOWLEDGEMENTS

We thank the editors and anonymous reviewers for helpful comments and guidance on previous drafts of this article. While this article was not directly funded, the authors acknowledge

ongoing support from the Natural Sciences and Engineering Council of Canada, the Social Sciences and Humanities Research Council of Canada, Genome Canada and the Canada Research Chairs program. D.G.R. is supported by the European Union's Horizon 2020 research and innovation programme under Marie Skłodowska-Curie grant agreement no. 838237-OPTIMISE.

CONFLICT OF INTEREST

The authors have no conflicts of interest.

AUTHORS' CONTRIBUTIONS

N.Y. conceptualized the manuscript and led the writing; D.G.R. contributed ideas, conducted the literature review and synthesis, and edited the manuscript; R.J.L., J.R.B. and S.J.C. contributed ideas and edited the manuscript.

DATA AVAILABILITY STATEMENT

This article does not use or report original or secondary data.

ORCID

Nathan Young https://orcid.org/0000-0002-2927-7025
Dominique G. Roche https://orcid.org/0000-0002-3326-864X
Robert J. Lennox https://orcid.org/0000-0003-1010-0577
Joseph R. Bennett https://orcid.org/0000-0002-3901-9513
Steven J. Cooke https://orcid.org/0000-0002-5407-0659

REFERENCES

Abraham, S., Beard, J., Manijacob, R. (2017). Remote environmental monitoring using internet of things (IoT). IEEE *Global Humanitarian Technology Conference*, San Jose, USA, 2017, pp. 1–6. https://doi.org/10.1109/GHTC.2017.8239335

Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. *Surveillance & Society*, *12*(2), 185–196.

Arts, K., van der Wal, R., & Adams, W. M. (2015). Digital technology and the conservation of nature. *Ambio*, *44*(4), 661–673.

August, T. A., Pescott, O. L., Joly, A., & Bonnet, P. (2020). AI naturalists might hold the key to unlocking biodiversity data in social media imagery. *Patterns*, *1*(7), 100116.

Ball, K., Haggerty, K. D., & Lyon, D. (Eds.). (2012). *Routledge handbook of surveillance studies*. Routledge.

Banzhaf, S., Ma, L., & Timmins, C. (2019). Environmental justice: The economics of race, place, and pollution. *Journal of Economic Perspectives*, *33*(1), 185–208.

Bennett, C. J. (2012). Privacy advocates, privacy advocacy and the surveillance society. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies Routledge handbook of surveillance studies* (pp. 412–420). Routledge.

Blumstein, D. T., Mennill, D. J., Clemins, P., … Kirschel, A. N. (2011). Acoustic monitoring in terrestrial environments using microphone arrays: Applications, technological considerations and prospectus. *Journal of Applied Ecology*, *48*(3), 758–767.

Borno, R. (2019). *Cisco connects to the conservation cause*. Cisco Blogs. Retrieved from https://blogs.cisco.com/csr/cisco-connects-to-the-conservation-cause

Brayne, S. (2020). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.

Butler, D., & Meek, P. (2013). Camera trapping and invasions of privacy: An Australian legal perspective. *Torts Law Journal*, *20*(3), 234–264.

Ceccaroni, L., Bibby, J., Roger, E., … Oliver, J. L. (2019). Opportunities and risks for citizen science in the age of artificial intelligence. *Citizen Science: Theory and Practice*, *4*(1), 29.

Chapman, A. D. (2020). *Current best practices for generalizing sensitive species occurrence data*. GBIF Secretariat. https://doi.org/10.15468/doc-5jp4-5g10

Cooke, S. J., Nguyen, V. M., Chapman, J. M., … Semeniuk, C. A. (2020). Knowledge co-production: A pathway to effective fisheries management, conservation, and governance. *Fisheries*, *46*(2), 89–97.

Cooke, S. J., Nguyen, V. M., Kessel, S., … Ford, A. T. (2017). Troubling issues at the frontier of animal tracking for conservation and management. *Conservation Biology*, *31*(5), 1205–1207.

Daume, S. (2016). Mining twitter to monitor invasive alien species — An analytical framework and sample information topologies. *Ecological Informatics*, *31*, 70–82.

Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation Biology*, *35*(2), 437–446.

Di Minin, E., Fink, C., Hiippala, T., & Tenkanen, H. (2019). A framework for investigating illegal wildlife trade on social media with machine learning. *Conservation Biology*, *33*(1), 210–213.

Dubrofsky, R. E., & Magnet, S. (2015). *Feminist surveillance studies*. Duke University Press.

Foucault, M. (1975). *Discipline and punish: The birth of the prison*. Vintage.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622.

Hussey, N. E., Kessel, S. T., Aarestrup, K., Cooke, S. J., Cowley, P. D., Fisk, A. T., … Whoriskey, F. G. (2015). Aquatic animal telemetry: A panoramic window into the underwater world. *Science*, *348*(6240), 1255642.

Jarić, I., Correia, R. A., Brook, B. W., … Kalinkat, G. (2020). iEcology: Harnessing large online resources to generate ecological insights. *Trends in Ecology & Evolution*, *35*(7), 630–639.

Kays, R., Sheppard, J., Mclean, K., … Crofoot, M. (2019). Hot monkey, cold reality: Surveying rainforest canopy mammals using drone-mounted thermal infrared sensors. *International Journal of Remote Sensing*, *40*(2), 407–419.

Lennox, R. J., Harcourt, R., Bennett, J. R., Davies, A., Ford, A. T., Frey, R. M., … Cooke, S. J. (2020). A novel framework to protect animal data in a world of ecosurveillance. *Bioscience*, *70*(6), 468–476.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill.

Lyon, D. (2010). Surveillance, power and everyday life. In P. Kalantzis-Cope & K. Gherab-Martín (Eds.), *Emerging digital spaces in contemporary society* (pp. 107–120). Palgrave Macmillan.

Macnish, K. (2017). *The ethics of surveillance: An introduction*. Routledge.

Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society*, *16*(2), 219–237.

Maritz, R. A., & Maritz, B. (2020). Sharing for science: High-resolution trophic interactions revealed rapidly by social media. *PeerJ*, *8*, e9485.

Marx, G. T. (1998). Ethics for the new surveillance. *The Information Society*, *14*, 171–185.

Marx, G. T. (2015). Surveillance studies. In J. D. Wright (Ed.), *International encyclopedia of the Social & Behavioral Sciences* (2nd ed.). Elsevier.

Mohanty, S. P., Hughes, D. P., & Salathé, M. (2016). Using deep learning for image-based plant disease detection. *Frontiers in Plant Science*, *7*, 1419.

Monahan, T. (2017). Regulating belonging: Surveillance, inequality, and the cultural production of abjection. *Journal of Cultural Economy*, *10*(2), 191–206.

Radjawali, I., & Pye, O. (2017). Drones for justice: Inclusive technology and river-related action research along the Kapuas. *Geographica Helvetica*, *72*, 17–27.

Resnik, D. B., Elliott, K. C., & Miller, A. K. (2015). A framework for addressing ethical issues in citizen science. *Environmental Science & Policy*, *54*, 475–481.

Rule, J. B. (2012). 'Needs' for surveillance and the movement to protect privacy. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 64–71). Routledge.

Sandbrook, C. (2015). The social implications of using drones for biodiversity conservation. *Ambio*, *44*, 636–647.

Sandbrook, C., Clark, D., Toivonen, T., Simlai, T., O'Donnell, S., Cobbe, J., & Adams, W. (2021). Principles for the socially responsible use of conservation monitoring technology and data. *Conservation Science and Practice*, *3*(5), e374.

Sandbrook, C., Luque-Lora, R., & Adams, W. M. (2018). Human bycatch: Conservation surveillance and the social implications of camera traps. *Conservation and Society*, *16*(4), 493–504.

Selod, S. (2018). *Forever suspect: Racialized surveillance of Muslim Americans in the war on terror*. Rutgers University Press.

Sharma, K., Fiechter, M., George, T., Young, J., Alexander, J. S., Bijoor, A., Suryawanshi, K., & Mishra, C. (2020). Conservation and people: Towards an ethical code of conduct for the use of camera traps in wildlife research. *Ecological Solutions and Evidence*, *1*(e12033), 1–6.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. NYU Press.

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2019). Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society*, *21*(3), 602–619.

Thompson, K. L., Lantz, T., & Ban, N. (2020). A review of indigenous knowledge and participation in environmental monitoring. *Ecology and Society*, *25*(2), 1–10.

Thylstrup, N. B. (2019). Data out of place: Toxic traces and the politics of recycling. *Big Data & Society*, *6*(2), 2053951719875479.

Trouille, L., Lintott, C. J., & Fortson, L. F. (2019). Citizen Science Frontiers: Efficiency, engagement, and serendipitous discovery with human–machine systems. *Proceedings of the National Academy of Sciences of the United States of America*, *116*(6), 1902–1909.

Tulloch, A. I., Auerbach, N., Avery-Gomm, S., Bayraktarov, E., Butt, N., Dickman, C. R., Ehmke, G., Fisher, D. O., Grantham, H., Holden, M. H., Lavery, T. H., Leseberg, N. P., Nicholls, M., O'Connor, J., Roberson, L., Smyth, A. K., Stone, Z., Tulloch, V., Turak, E., … Watson, J. E. M. (2019). A decision tree for assessing the risks and benefits of publishing biodiversity data. *Nature Ecology & Evolution*, *2*(8), 1209–1217.

Wearn, O. R., Freeman, R., & Jacoby, D. M. P. (2019). Responsible AI for conservation. *Nature Machine Intelligence*, *1*(2), 72–73.

Wetzel, C. (2020). *3-D printed sea turtle eggs reveal poaching routes*. Smithsonian Magazine. Retrieved from https://www.smithsonianmag.com/science-nature/3-d-printed-sea-turtle-eggs-reveal-poaching-routes-180975991/

Wich, S. A., & Koh, L. P. (2018). *Conservation drones: Mapping and monitoring biodiversity*. Oxford University Press.

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile.

SUPPORTING INFORMATION

Additional supporting information may be found in the online version of the article at the publisher's website.

How to cite this article: Young, N., Roche, D. G., Lennox, R. J., Bennett, J. R., & Cooke, S. J. (2022). Ethical ecosurveillance: Mitigating the potential impacts on humans of widespread environmental monitoring. *People and Nature*, *4*, 830–840. https://doi.org/10.1002/pan3.10327