

Truth from the sewage: are we flushing privacy down the drain?

Bart van der Sloot*

Abstract

Wastewater is a new source of information being harvested in the fight against a wide range of phenomena, such as cancer, drug production, and Covid19. Law enforcement agencies monitor sewage systems to locate buildings where XTC and amphetamines are produced. Smart toilets allow citizens to analyse their faeces for prevalent diseases. National Health Institutes monitor wastewater to alert them of early virus outbreaks. Given the wealth of information that can be harvested, sewage monitoring might become one of the most common and invasive forms of surveillance in the coming years. Although potentially problematic in light of the right to privacy and data protection, it is unclear whether and to what extent the various forms of sewage monitoring would fall under the material scope of these rights. In addition, if they would, the question is whether they would be prohibited or would meet the various requirements entailed in the relevant legal instruments.

Keywords: Sewage Surveillance; Smart Toilets; Data Protection; Privacy; ECHR; GDPR.

1. Introduction

Sewage monitoring is not entirely new and the information that can be extracted from wastewater¹ has grown exponentially in recent years. Wastewater has been filtered for decades, both to prevent environmental harm by filtering dangerous fluids such as acids from the water before being discharged in a river or ocean and to prevent health risk to citizens by cleaning water before it is recycled as tap water. Wastewater facilities monitor water quality constantly to assess whether water should be purified. New techniques and sensors have been introduced that can measure various types of substances in the water. On a population level, this can yield information about drug and medicine use,

* Associate Professor, Tilburg Institute for Law, Technology and Society (TILT), Tilburg University.

¹ For the purposes of this paper, wastewater will broadly refer to anything that is disposed of through the sewage, and to a lesser extent, to liquids or materials that are disposed by drainage to rivers or other natural waters.

environmental pollution, and about health and dietary trends.² Through data analysis, alarm can be raised when a nearby factory has leaked dangerous substances in the environment, when XTC³ production is significantly higher in certain areas than in others, or when virus outbreaks are visible in the wastewater of specific cities.⁴ In addition, monitoring technologies have become increasingly precise. Sewage monitoring is no longer limited to assessing the wastewater of neighbourhoods, cities, or larger areas. Robots enable authorities to analyse wastewater releases under specific facilities and buildings, including private dwellings.

This phenomenon raises many complex issues in light of the right to privacy and data protection. For example, to which point is the sewage to be considered part of a person's home; are water samples containing peoples' stool to be considered biometric and identifiable personal data; are faeces protected under the concept of bodily integrity; and to what extent can untargeted sewage monitoring be likened to mass surveillance on the internet? In addition, there are questions on the legitimacy of the various types of sewage monitoring. For example, there is often a complex web of players involved. Municipalities manage and control sewages under cities and wastewater facilities are often private organisations. Moreover, law enforcement agencies and National Health Institutes are public sector departments, and sewage systems are often partly owned by citizens or housing associations. A key question is, which organisation has authority to conduct sewage analysis and to what extent can they share and re-use the data therein for different purposes?

This article will introduce the reader to the aforesaid and other questions. Section 2 describes the various forms of sewage monitoring. Section 3 discusses the material scope of the rights to privacy and data protection vis-à-vis sewage monitoring. Section 4 analyses the legitimacy of several applications and use cases and section 5 will provide a conclusion. The goal of this article is to provide a preliminary overview of this new technology and introduce the reader to the many difficult legal questions that are raised by the various forms of sewage monitoring.

2. Sewage monitoring

In its most basic form, sewage monitoring is used for measuring environmental pollution and its origins. *'Sewage are the method used to check on hazardous release of gaseous components into the environment in areas. Due to natural decomposition it often leads to production of toxic gases. These gases can be poisonous if inhaled for a long period of time.'*⁵ Wastewater analysis can be used, inter alia, for *'quality controls in a river, aqua*

² Liu, C., Li, H., & Zhang, Q. (2020). Research on Sewage Monitoring and Water Quality Prediction Based on Wireless Sensors and Support Vector Machines. *Wireless Communications and Mobile Computing*, 2020.

³ Short for ecstasy, also known as Methylenedioxyamphetamin (MDMA).

⁴ Li, T., Winnel, M., Lin, H., Panther, J., Liu, C., O'Halloran, R., & Zhao, H. (2017). A reliable sewage quality abnormal event monitoring system. *Water research*, 121, 248-257.

⁵ Dharshini, V. P., Merin Mathew, M., Leena, S., & Nandhini, A. Smart Sewage Gas Detection and Monitoring using IoT. *International Journal of Research in Engineering, Science and Management* Volume-3(3), March-2020

culture outlets or “off shore” fish cages’,⁶ to prevent industrial waste leakages from entering water used to irrigate farm lands or to ensure that tap water is clean and can be consumed without danger.⁷

Currently, sewage monitoring is deployed as a way to map Covid19 and detect early outbreaks as excrement may contain traces of the virus or antibodies produced by the body even before the patient shows signs of illness. In addition, so called asymptomatic patients, patients that show no outward symptoms of the disease, can be mapped. The technique for tracing particles is becoming increasingly precise. *‘We estimate if there’s one person infected in a population of 10 000, we can pick it up—it’s that sensitive.*’⁸ However, had sewage monitoring been used earlier, outbreaks might have been prevented. For example, analysing wastewater from Italian cities indicates that SARS-CoV-2, responsible for Covid19, was already present on December 18, 2019, in cities such as Turin and Milan, more than two months before the first outbreaks were reported on February 21, 2020.⁹ Not surprisingly, many countries are investing in this type of sewage monitoring.¹⁰ Not only is this form of monitoring considered effective, precise and relatively cheap, it is also understood to be *‘a non-invasive warning approach to alert communities to new COVID-19 infections, given that most people will not be tested.*’¹¹ Yet, in comparison, the method of normal Covid-19 tests, is to penetrate citizens’ throat and/or nose with a cotton swab, but such bodily penetration is not needed with sewage monitoring.

These applications fit into the broader trend to analyse biomarkers in sewage water for population health screenings, or what is called *‘sewage epidemiology*’.¹² Certain types of

⁶ Gallardo-Gonzalez, J., Baraket, A., Boudjaoui, S., Metzner, T., Hauser, F., Rößler, T. & Bausells, J. (2019). A fully integrated passive microfluidic Lab-on-a-Chip for real-time electrochemical detection of ammonium: Sewage applications. *Science of The Total Environment*, 653, 1223-1230.

⁷ Martins, C. C., Aguiar, S. N., Wisnieski, E., Ceschim, L. M., Figueira, R. C., & Montone, R. C. (2014). Baseline concentrations of faecal sterols and assessment of sewage input into different inlets of Admiralty Bay, King George Island, Antarctica. *Marine pollution bulletin*, 78(1-2), 218-223.

⁸ Baraniuk, C. (2020). Sewage monitoring is the UK’s next defence against covid-19. *bmj*, 370.

⁹ La Rosa, G., Mancini, P., Ferraro, G. B., Veneri, C., Iaconelli, M., Bonadonna, L. & Suffredini, E. (2020). SARS-CoV-2 has been circulating in northern Italy since December 2019: evidence from environmental monitoring. *Science of the Total Environment*, 750, 141711.

¹⁰ <<https://www.rivm.nl/en/covid-19/sewage>>.

¹¹ Orive, G., Lertxundi, U., & Barcelo, D. (2020). Early SARS-CoV-2 outbreak detection by sewage-based epidemiology. *Science of The Total Environment*, 139298.

¹² See for the use of this term inter alia: Van Nuijs, A. L., Mougél, J. F., Tarcomnicu, I., Bervoets, L., Blust, R., Jorens, P. G., ... & Covaci, A. (2011). Sewage epidemiology—a real-time approach to estimate the consumption of illicit drugs in Brussels, Belgium. *Environment international*, 37(3), 612-621. van Nuijs, A. L., Abdellati, K., Bervoets, L., Blust, R., Jorens, P. G., Neels, H., & Covaci, A. (2012). The stability of illicit drugs and metabolites in wastewater, an important issue for sewage epidemiology?. *Journal of hazardous materials*, 239, 19-23. Prichard, J., Hall, W., de Voogt, P., & Zuccato, E. (2014). Sewage epidemiology and illicit drug research: the development of ethical research guidelines. *Science of the Total Environment*, 472, 550-555. Baker, D. R., Očenášková, V., Kvalcova, M., & Kasprzyk-Hordern, B. (2012). Drugs of abuse in wastewater and suspended particulate matter—further developments in sewage epidemiology. *Environment international*, 48, 28-38.

viruses can be detected easily in sewage water,¹³ so can nutrient inputs,¹⁴ pathogens,¹⁵ pharmaceuticals, and antibiotics.¹⁶ In addition, *'analyses of sewage samples have the potential to be used for population-level surveillance of antibiotic-resistant pathogens in a cost-efficient way. The approach might then complement current monitoring systems by resolving some of the problems associated with the limited sampling in clinical praxis and be applied to provide antibiotic resistance data and possibly guide empirical treatment recommendations in countries and regions where surveillance is currently very scarce or completely lacking.'*¹⁷ Yet, wastewater analysis can also point to underlying causes of diseases, ill-health, dysfunction, stress, trauma, or injury, and xenobiotics, such as nutritive constituents, active pharmaceutical ingredients, and contaminants in food.¹⁸ Moreover, sewage monitoring is *'currently being used to provide more current monitoring data on community-wide use of illicit drugs, drugs of abuse, tobacco, and alcohol.'*¹⁹

Many smart city projects and living labs analyse population and individual health through sewage surveillance.²⁰ For example, the MIT Underworlds project's²¹ slogan is *'A vast reservoir of information on Human Health and Behaviour Lives in our Sewage. And this*

¹³ Meleg, E., Bányaí, K., Martella, V., Jiang, B., Kocsis, B., Kisfali, P., ... & Szűcs, G. (2008). Detection and quantification of group C rotaviruses in communal sewage. *Applied and environmental microbiology*, 74(11).

¹⁴ Gorman, D., Turra, A., Connolly, R. M., Olds, A. D., & Schlacher, T. A. (2017). Monitoring nitrogen pollution in seasonally-pulsed coastal waters requires judicious choice of indicator species. *Marine Pollution Bulletin*, 122(1-2), 149-155.

¹⁵ Sinclair, R. G., Choi, C. Y., Riley, M. R., & Gerba, C. P. (2008). Pathogen surveillance through monitoring of sewer systems. *Advances in applied microbiology*, 65, 249.

¹⁶ Oertel, R., Schubert, S., Mühlbauer, V., Büttner, B., Marx, C., & Kirch, W. (2014). Determination of clindamycin and its metabolite clindamycin sulfoxide in diverse sewage samples. *Environmental Science and Pollution Research*, 21(20), 11764-11769. Pérez, S., Eichhorn, P., & Aga, D. S. (2005). Evaluating the biodegradability of sulfamethazine, sulfamethoxazole, sulfathiazole, and trimethoprim at different stages of sewage treatment. *Environmental Toxicology and Chemistry: An International Journal*, 24(6), 1361-1367.

¹⁷ Hutinel, M., Huijbers, P. M. C., Fick, J., Åhrén, C., Larsson, D. G. J., & Flach, C. F. (2019). Population-level surveillance of antibiotic resistance in *Escherichia coli* through sewage analysis. *Eurosurveillance*, 24(37), 1800497.

¹⁸ See inter alia: Kinney, C. A., Furlong, E. T., Zaugg, S. D., Burkhardt, M. R., Werner, S. L., Cahill, J. D., & Jorgensen, G. R. (2006). Survey of organic wastewater contaminants in biosolids destined for land application. *Environmental science & technology*, 40(23), 7207-7215. Fu, Q., Malchi, T., Carter, L. J., Li, H., Gan, J., & Chefetz, B. (2019). Pharmaceutical and personal care products: From wastewater treatment into agro-food systems. Cuellar-Bermudez, S. P., Aleman-Nava, G. S., Chandra, R., Garcia-Perez, J. S., Contreras-Angulo, J. R., Markou, G., ... & Parra-Saldivar, R. (2017). Nutrients utilization and contaminants removal. A review of two approaches of algae and cyanobacteria in wastewater. *Algal Research*, 24, 438-449. Gatica, J., & Cytryn, E. (2013). Impact of treated wastewater irrigation on antibiotic resistance in the soil microbiome. *Environmental Science and Pollution Research*, 20(6), 3529-3538.

¹⁹ Daughton, C. G. (2018). Monitoring wastewater for assessing community health: Sewage Chemical-Information Mining (SCIM). *Science of The Total Environment*, 619, 748-764.

²⁰ <https://www.cost.eu/?s=sewage>

²¹ Reis-Castro, L. (2017). The Underworlds Project and the "Collective Microbiome": Mining Biovalue From Sewage. In *Bioeconomies* (pp. 105-127). Palgrave Macmillan, Cham.

resource is untapped. ‘Rather than sampling sewage downstream at the wastewater treatment plant, Underworlds samples upstream throughout the sewage network in the city to develop individual readings of particular neighborhoods.’²² This is done by having robots enter the sewage system and monitoring the wastewater under specific premises or neighbourhoods. The promise of the ‘smart sewage’ is that it could impact the way non-communicable diseases are studied because biomarkers for diseases such as obesity and diabetes can be measured at unprecedented scale and temporal resolution. Some of these robots are now equipped with ‘Intelligent Real Time Diagnostic System’ that allow for real time analysis of excrement.²³ Such systems may also be used, for example, to measure how many citizens there are in a designated area or building.²⁴ Ultimately, if biomarkers and excrement are processed on an individual level, they may track individuals’ eating pattern, whereabouts, and movements across the map.²⁵

Like monitoring wastewater on a population level in smart cities, smart homes can be equipped with a so-called ‘smart toilets’ to allow citizens to monitor their individual health. The smart toilet is a toilet that can analyse stool for diseases, infections, and nutrient diets.²⁶ This can be done both by analysing liquids,²⁷ as well as by analysing the gasses, and odour, a person produces.²⁸ Data analysis can be used for medical diagnostics and for screening diseases such as diabetes mellitus, bladder infections, kidney failure,²⁹ or for giving nutritional advice.³⁰ These types of toilets can also detect ‘*who is using the toilet from a fingerprint scanner on the flush handle, and “anal prints” – distinctive creases in the lining of the anus, captured by video frames.*’³¹

²² <http://underworlds.mit.edu/>

²³ Gaska, K., & Generowicz, A. (2020). SMART Computational Solutions for the Optimization of Selected Technology Processes as an Innovation and Progress in Improving Energy Efficiency of Smart Cities—A Case Study. *Energies*, 13(13), 3338.

²⁴ Abbas, O., Abou Rjeily, Y., Sadek, M., & Shahrour, I. (2017). A large-scale experimentation of the smart sewage system. *Water and Environment Journal*, 31(4), 515-521.

²⁵ Abou Rjeily, Y., Sadek, M., Chehade, F. H., Abbas, O., & Shahrour, I. (2017, September). Smart system for urban sewage: Feedback on the use of smart sensors. In 2017 Sensors Networks Smart and Emerging Technologies (SENSET) (pp. 1-4). IEEE. Abbas, O., Abou Rjeily, Y., Sadek, M., & Shahrour, I. (2017). A large-scale experimentation of the smart sewage system. *Water and Environment Journal*, 31(4), 515-521.

²⁶ Mohanty, M. D., & Mohanty, M. N. (2019). A cognitive approach for design of smart toilet in healthcare units. In *Cognitive Informatics and Soft Computing* (pp. 771-780). Springer, Singapore.

²⁷ Bae, J. H., & Lee, H. K. (2018). User health information analysis with a urine and feces separable smart toilet system. *Ieee Access*, 6, 78751-78765.

²⁸ Choden, P., Seesaard, T., Dorji, U., Sriphrapadang, C., & Kerdcharoen, T. (2017, June). Urine odor detection by electronic nose for smart toilet application. In 2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) (pp. 190-193). IEEE.

²⁹ <<https://gizmodo.com/health-monitoring-smart-toilet-remembers-your-distinct-1842726039>>.

³⁰ <<https://www.intercleanshow.com/news/articles/washroom-innovation-smart-toilets/>>.

³¹ <<https://www.theguardian.com/society/2020/apr/06/magic-toilet-could-monitor-users-health-say-researchers>>.

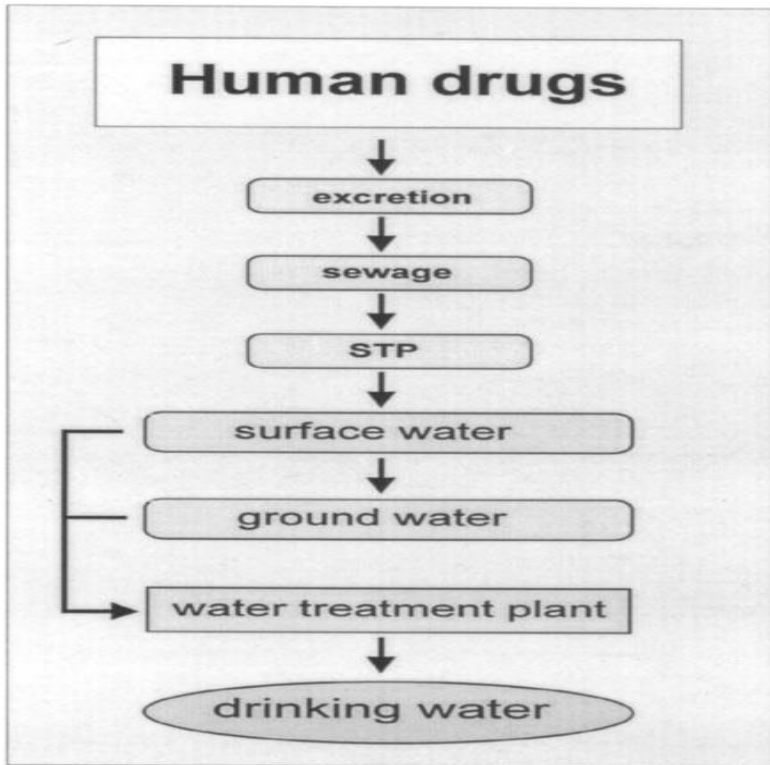


Figure 1: clinical sewage surveillance³²

When installed in public buildings, smart toilets could make a wealth of information about individual citizens available to governmental organisations, restaurants, etc. Besides so called 'clinical sewage surveillance',³³ a new form of 'criminal sewage surveillance' is on the rise; sewage monitoring can be used to detect illegal substances or waste material that are residual to the production of drugs. In countries such as Germany, the Netherlands, and Poland, illegal chemical drugs are increasingly produced by individuals in their homes,

³² Picture taken from: Stumpf, M., Ternes, T. A., Wilken, R. D., Rodrigues, S. V., & Baumann, W. (1999). Polar drug residues in sewage and natural waters in the state of Rio de Janeiro, Brazil. *Science of the total environment*, 225(1-2), 135-141.

³³ Barril, P. A., Giordano, M. O., Isa, M. B., Masachessi, G., Ferreyra, L. J., Castello, A. A., ... & Nates, S. V. (2010). Correlation between rotavirus A genotypes detected in hospitalized children and sewage samples in 2006, Córdoba, Argentina. *Journal of medical virology*, 82(7), 1277-1281.

sheds, and barns.³⁴ When drug production waste is flushed down the toilet, this might have a significant environmental impact, might damage the sewage system itself and might incapacitate water facilities when producing drinkable tap water. Criminal sewage surveillance comes in various forms and degrees of precision.³⁵ At the water treatment facility, wastewater may be checked for substances. Usually, a wastewater facility processes water from several areas and cities, so that general population information may be obtained. For example, data analysis may indicate that drug consumption or production of XTC is rising, while the speed of production of other designer drugs are declining. This may inform law enforcement agencies when developing strategies and setting investigatory priorities.

Sewages can be assessed on city, neighbourhood, or street level. This allows law enforcement agencies to narrow down areas of drug production or consumption. If sewage analysis of city A indicates high levels of drug waste, a more detailed map may be produced to locate which neighbourhood(s) are most responsible. Subsequently, such analysis may be done on street level, though what complicates matters is that for both drug consumption and drug use, there is generally no constant flow of drug waste. For example, with the production of chemical drugs, waste material may be flushed down the drain once a week or even once a month, if reservoirs are big enough. That is why, if there is suspicion about a specific home or facility being the locus of drug waste, robots may enter the sewage to monitor wastewater directly under that home or facility.³⁶ Besides these targeted forms of sewage surveillance, sewage monitoring can also be applied in untargeted ways. In this case, a robot floats in the sewage system permanently and when receiving indicators of drug use or production, it will track the location of the source.³⁷

³⁴ Škorvánek, I., Koops, B. J., & Timan, T. (2019). Surveillance, Criminal Procedure, and Regulatory Connection: the Case of Sewage Monitoring. *Tilburg Law School Research Paper Forthcoming*.

³⁵ Škorvánek, I., Koops, B. J., & Timan, T. (2019). Surveillance, Criminal Procedure, and Regulatory Connection: the Case of Sewage Monitoring. *Tilburg Law School Research Paper Forthcoming*.

³⁶ <http://micromole.eu/advanced-in/low-cost-sampling-and-storage-integrated-system/>

³⁷ <http://micromole.eu/advanced-in/chemical-sensors-and-specificity/>

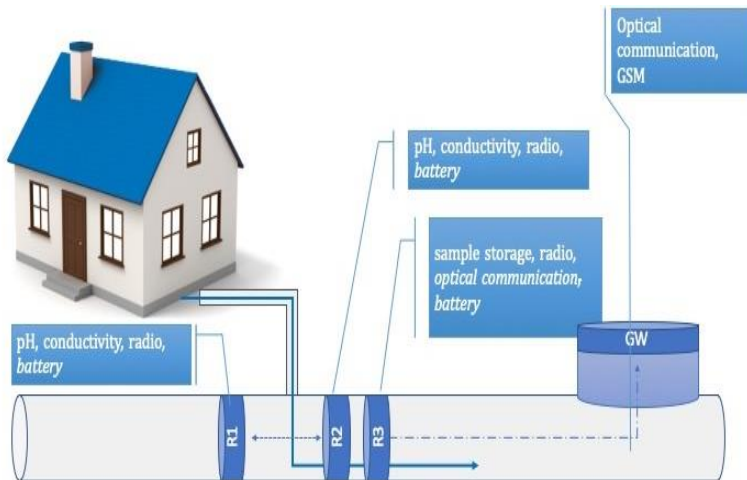


Figure 2: remote targeted sewage monitoring³⁸

3. Applicability of the right to data protection

The right to data protection is protected through Article 8 of the European Charter of Fundamental Rights³⁹ and is further specified in the General Data Protection Regulation (GDPR).⁴⁰ Processing by law enforcement agencies is regulated through the so called Law Enforcement Directive.⁴¹ It is clear that some forms of sewage surveillance will fall under the material scope of the right to data protection, such as when person A lives alone and installs a smart toilet in her home and her stool is analysed for nutrient advice or detection of diseases before it enters the sewage. However, for most other scenarios, it is substantially more difficult whether, and if so, to what extent this will be. This section will touch upon a number of potential questions on the material scope of the right to data protection vis-à-vis sewage monitoring.

³⁸ <http://micromole.eu/advanced-in/low-power-remote-monitoring/>

³⁹ Charter of Fundamental Rights of the European Union, 2012/C 326/02 < <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>>.

⁴⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

⁴¹ Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

First, when a smart toilet is installed in a home with more than one resident, the matter of applicability already becomes more complex. Although smart toilets should be able to determine which person is using the toilet on the basis of her 'anal print', the dark equivalent of the 'fingerprint', it is currently unclear how precise this identification method is and to what extent anal prints are as stable as fingerprints. *The device also has a built-in recognition system to ensure the identity of the person using the toilet. This system is based on the biological uniqueness of each person's anal print, analogous to dermatoglyphic characteristics or fingerprints that differ even in MZ twins. It was necessary to have this feature in the event that a person using the toilet is not the person who flushes. Features of the toilet are still being tested. An informative and fascinating addition to this project would involve pairs of MZ [Monozygotic] and DZ [Dizygotic] twins. This would allow searching for markers of genetically influenced diseases and determining whether the device could distinguish the anal prints of MZ co-twins.*⁴² Currently, it is uncertain whether this identification technique is sufficiently precise to consider the data obtained through it 'personal data' for the purposes of the GDPR, as it is developed by one research team around the world only and no underlying data supporting its effectiveness and accuracy have been produced. Yet, if sufficiently precise, either now or after further improvements have been implemented, identification through anal prints may be a new and inescapable form of gathering personal data.

Second, it should be kept in mind that faeces themselves are often unreliable individual identifiers. This is because their substance changes according to a person's diet, intake, and exogenous factors,⁴³ it is often unknown who a potential DNA profile belongs to. Suppose smart toilets would be installed in public facilities, such as governmental buildings, business premises, hotels, pubs or theatres, it will be unknown which of the employees or visitors is using the toilet and is providing the faecal input. However, this may differ when wastewater analysis is combined with other forms of identification, such as cameras, whether or not equipped with facial recognition software. Most jurisdictions around the world do not allow organisations to monitor inside restrooms, but there is generally no such prohibition on surveying outside restrooms, including monitoring those who enter such facilities. This means that when there is only one toilet inside a restroom, the stool of a person may be linked to an individual person.

⁴² Segal, N. L. (2020). COVID-19: Twin Research in Progress/Twin Research Reviews: Asthmatic and Nonasthmatic Twins; Stanford University Study of Anal Prints; Twin Mammals and COVID-19; Twin Delivery and the Three 'Rs'/Mixed Media: The Rainman Twins—The Film; Twins Irish Pub; Twins 'Covid and Corona'; Death of a Surgeon Who Separated Conjoined Twins; Twinco—Twin-Based Supply Company. *Twin Research and Human Genetics*, 23(4), 259-263.

⁴³ See inter alia: Mercan, S., Kuloglu, M., & Ascioglu, F. (2019). Monitoring of illicit drug consumption via wastewater: development, challenges, and future aspects. *Current Opinion in Environmental Science & Health*, 9, 64-72. Anand, U., Adelodun, B., Pivato, A., Suresh, S., Indari, O., Jakhmola, S., ... & Di Maria, F. (2021). A review of the presence of SARS-CoV-2 RNA in wastewater and airborne particulates and its use for virus spreading surveillance. *Environmental Research*, 110929. Walker, N. L., Norton, A., Harris, I., Williams, A. P., & Styles, D. (2019). Economic and environmental efficiency of UK and Ireland water companies: Influence of exogenous factors and rurality. *Journal of environmental management*, 241, 363-373.

Third, when more than one toilet is inside a restroom, identification would in principle be difficult. This means that in principle, in such use cases, stool analysis will not fall under the material scope of the right to data protection.⁴⁴ This may be different, however, when the results of the analysis are either directly communicated to the user, e.g. giving her dietary or medical advice, such as done at certain music festivals.⁴⁵ Alternatively, this may be the case when the results are used to make decisions, such as when a person with high blood pressure is asked to leave the amusement park because it fears heart failure when that person would use one of its roller-coaster. An example would be when a non-identified person goes to the toilet in an amusement park and the toilet automatically warns that person that she should leave the park immediately after their stool has been analysed. In principle, when data is used to make decisions about a person, even although their exact identity is unknown, the data is to be considered as personal data.⁴⁶

Fourth, going back to the scenario in which multiple family members use one smart toilet, it might be argued that even in such a case, the toilet would be processing personal data using the analogy with a personal computer used by multiple family members. The former Article 29 Working Party has suggested that when a cookie is placed on such a computer, or when the IP-address is used, for example, for behavioural advertising, this is considered to fall under the data protection regime even although the cookie is processing personal data by 4 or 5 family members.⁴⁷ The Working Party even suggested that this might be true for public computers. *'A particular case would be that of some sorts of IP addresses which under certain circumstances indeed do not allow identification of the user, for various technical and organizational reasons. One example could be the IP addresses attributed to a computer in an internet café, where no identification of the customers is requested. It could be argued that the data collected on the use of computer X during a certain timeframe does not allow identification of the user with reasonable means, and therefore it is not personal data. However, it should be noted that the Internet Service Providers will most probably not know either whether the IP address in question is one allowing identification or not, and that they will process the data associated with that IP in the same way as they treat information associated with IP addresses of users that are duly registered and are*

⁴⁴ The GDPR speaks of the 'means reasonable likely to be used for identification. 'To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.' Recital 26 GDPR. This means that whether a person is or is not identifiable depends on the circumstances of the case. It is not excluded that when several people use one toilet, they may be identified individually, potentially with the use of other means of identification. See also: Party, Data Protection Working. "Opinion 05/2014 on Anonymisation Techniques." (2014).

⁴⁵ <<https://www.imec-int.com/en/the-netherlands/smart-toilet>>.

⁴⁶ Working Party 29, Opinion 4/2007 on the concept of personal data, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

⁴⁷ See also: Court of Justice, Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland, 19 October 2016, ECLI:EU:C:2016:779.

*identifiable. So, unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side.*⁴⁸ Consequently, in this analogy, it could be argued that this would also apply to a toilet shared by one household, and potentially, one that is used by many unspecified persons in a public facility. The question is whether the toilet owner, the operator of the building, or the facility where the toilet is located, and/or the sewage system operator knows who is using the toilet. It can also concern whether they know for certain that the individuals using it cannot be identified because many times, such will be uncertain or depend on the circumstances of each particular case, the Working Party suggests erring on the safe side and treat all data as personal data.

However, there are two important differences. First, IP addresses are commonly used as direct actionable knowledge by advertisers – an IP address used to search for term A will receive advertisement A1 – while this is not the case for most use cases of smart toilets. Apart from use cases in which direct feedback is given or direct action is taken upon stool analysis, most forms of sewage monitoring can be used to identify patterns. This can be done either on an individual level, e.g., that a person's blood pressure is high is something that cannot be determined on the basis of one measurement,⁴⁹ because high blood pressure at one specific moment might be caused by energy intensive activities. Or on an aggregate level, e.g., 70% of the visitors of this music festival have used XTC. Second, the level of precision is highly important to smart toilets, while this is not the case for personal advertisements. If a personal computer is used to search for purple pumps and fishing gear, advertisements may be simply shown of both types of products. The expected click rate, the number of times users click on the advertisement, being low, personal advertisements' main promise is to make advertisements somewhat more tailored and not to target persons with surgical precision. This is different for smart toilets. It is impossible to give dietary advice or do a medical analysis if it is unknown whether of the say 20 toilet uses, 5 are by person A (20 years old, eating healthy), 5 are by person B (30 years old, eating relatively healthy) and 10 are by person C (60 years old, with a bad eating habit) or that these are all by the same person, with fluctuating levels of dietary healthiness.

Fifth, the problem becomes even more complex when excrement is not analysed before it enters the sewage system, but just after, such as when a robot is placed in the sewage system under a particular home. This is a use case developed by law enforcement agencies for criminal investigations concerning drug consumption or production. Faeces contain traces of drug use and the waste material of the production of chemical drugs is often flushed down the drain. Such a robot is designed to measure certain substances related to drug consumption or production constantly, and when these substances are found, to take two or more samples of the wastewater. One of these robots, is called Micromole. *'The micromole system is able to periodically measure pH and conductivity of the sewage flow and to trigger the sampling module for physical evidence gathering, whenever the pH and*

⁴⁸ Ibid.

⁴⁹ Which of course does not mean that an amusement park could not act on an individual measurement anyway.

*conductivity measurements abruptly change as to match values that can be correlated with an ATS [Amphetamine-Type Stimulants] waste spill in the sewage.*⁵⁰

It is unclear whether these samples would be permissible and acceptable as evidence in criminal proceedings for three reasons. First, these systems are often imprecise. Second, the analysis of the samples is an irreversible process. Third, especially with drug production, the samples only contain waste material, but do not indicate who flushed that material down the sewage. Consequently, these types of monitoring may be less suitable for collecting hard evidence.⁵¹ However, they can be used for meeting the threshold of having a ‘reasonable suspicion’ which is usually required when the police want to enter a building. Such may be the case, for example, when sewage monitoring has established the discharge of prohibited substances or material that could indicate drug production under a specific home and law enforcement officers want to enter a building to verify that suspicion and to collect evidence that is admissible in court.

In light of the right to data protection, similar arguments would apply. The fact that a toilet is used to discharge waste material does not indicate who is responsible for that action, let alone who is responsible for the drug production process. Obviously, under certain circumstances, such might lead to identifiable data, when only one person has access to the facility or toilet. Similarly, when flushing the toilet, urine and/or faeces mingles with water, cleaning products that are used in the toilet, and left-over material from previous users. In addition, chemical toilets add chemicals before draining the wastewater in the sewage. Consequently, although sewage analysis might indicate that a sample contains both traces of prohibited substance A and DNA of person B, it is incapable of providing with certainty that person B used substance A. Whether such data analysis – linking prohibited substance A to person B – will be considered the processing of ‘personal data’ for the purposes of the GDPR will depend on the circumstances of the case. Yet, it seems likely that if such analysis is used as actionable knowledge, either by the police, the sewage system operator, or another organisation, such will be considered to fall under the scope of the EU data protection regime.

Sixth, it might be argued that biological material gathered by such tools themselves should be considered personal data. Indeed, the European Court of Human Rights (‘ECtHR’), in the Marper case, found that DNA and biological material may indeed be considered ‘personal data’.⁵² It stressed that *‘all three categories of the personal information retained by the authorities in the present case, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals.’*⁵³ Consequently, it could be argued that either anal prints or the excrement itself could be considered personal data. But as Lee

⁵⁰ <<http://micromole.eu/advanced-in/low-power-remote-monitoring/>>.

⁵¹ See for a more elaborate discussion: Škorvánek, I., Koops, B. J., & Timan, T. (2019). Surveillance, Criminal Procedure, and Regulatory Connection: the Case of Sewage Monitoring. Tilburg Law School Research Paper Forthcoming.

⁵² Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 28 January 1981; in force 1 October 1985) ETS 108

⁵³ S and Marper v United Kingdom (App no 30562/04 and 30566/04) ECtHR, 4 December 2008

Bygrave explains, the conclusion of the ECtHR seems to apply only to that case and cannot be interpreted as providing a general legal principle.⁵⁴

In addition, he suggests that there are both arguments against treating bodily material itself as 'personal data' and in favour. His interpretation of 'personal data' *'prevents samples as such being treated as 'information', since the latter has a cognitive dimension involving comprehension of what is represented by data. Further, treating data as essentially a formalised representation of objects or processes makes it difficult to view the body itself as data. Yet while difficult, it is perhaps not impossible. Although the entire physical body of a person can scarcely be assimilated within the notion of 'data' as a representation of (aspects of) that person, could not parts of the body be so assimilated?'*

⁵⁵ In Bygrave's opinion, it can be argued that biological material which has been separated from a person's body and structured as a sample or set of samples with the intention of providing information can function at the very least analogously to data. This means that under this interpretation, the conceptual barriers to treating biological material as data are not as profound as is sometimes assumed. Although consequently, it cannot be excluded that excrement itself could be considered 'personal data', this is uncertain. For example, when biological material of a person is gathered through sewage monitoring under a public building, but there is no way of linking that material to a specific person, it is unlikely that such will be considered 'personal data'. This should be treated analogous to when a fingerprint or limb of a person is found, without there being a possibility to establish whom it belongs to.

Seventh, under the General Data Protection Regulation, a special regime applies to the processing of biometric data: *'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'*.⁵⁶ It could be argued that like finger prints, anal prints should be considered biometric data when the technique would be sufficiently precise to allow for individual identification. But here, there is difficulty too. For example, Catherine Jasserand explains that biological material itself should not be considered biometric data, only the identifying data pattern that is distilled from that raw material. *'Some authors, as well as the Article 29 WP, wrongly use the phrase 'raw (biometric) data' to designate a biometric sample. Raw (biometric) data are, for example, a fingerprint, fingertip, iris, voice, etc. In the absence of any technical processing through which the raw data are obtained, these fall outside the scope of biometric data. The term 'raw data' should only be used as a synonym of biometric characteristics.'*⁵⁷ Whether the patterns and templates should be considered

⁵⁴ Bygrave, L. A. (2015). Information concepts in law: Generic dreams and definitional daylight. Oxford Journal of Legal Studies, 35(1), 91-120.

⁵⁵ Bygrave, L. A. (2010). The body as data? Biobank regulation via the 'Back Door' of data protection law. Law, Innovation and Technology, 2(1), 1-25. See also: Bygrave, L. A. (2012). The data difficulty in database protection. University of Oslo Faculty of law research paper, (2012-18).

⁵⁶ Article 4 (14) GDPR.

⁵⁷ Jasserand, C. A. (2016). Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective. International Data Privacy Law, 6(1), 63-76.

personal data depends on the question whether they can be linked to a specific individual. Again, as was discussed previously, this depends on the exactitude with which a sample can be linked to a specific individual, which will be the case only in a limited number of use case scenarios.⁵⁸

Eighth, it could be argued that although no exact information can be derived from sewage monitoring, the Working Party 29 has suggested that opinions and subjective beliefs will fall under the scope of the EU data protection regime when linked to a specific person.⁵⁹ Thus, even if an organisation makes an educated guess or incorrect assumption about a person, such as when a health insurer incorrectly assumes that a person is using drugs, and takes action accordingly, or the police incorrectly believes a building is used for drug production, and searches that building, such will be considered personal data.

Ninth, when decisions are made on general or statistical information, such will be treated as falling under the EU data protection framework when they have an impact on an individual person or small group.⁶⁰ A question that cannot be answered in abstract is whether the GDPR applies if decisions made on group or neighbourhood level. For example, when a law enforcement authority surveys a specific neighbourhood to find potential suspects, after sewage monitoring has indicated that drug production is likely to take place in that neighbourhood, the question may arise whether that information (that drug production is likely to take place in a specific neighbourhood) in itself qualifies as personal data. Such will depend on the impact and the size of the group the data concerns. Thus, if there are only two houses in the area that is surveyed (e.g. a remote area in the periphery of the country), such may be the case, while if there are 1.000 homes, the GDPR will generally not apply to statistical data about that area.

Finally, reference can be made to what is called the ‘composition effect’ in light of informational privacy and data protection. For example, one set of data may not in itself reveal any personal data. However, when several datasets that in themselves do not contain information that may be linked to a specific person are combined, a detailed personal profile may arise. *‘Composition effects can take many forms. For instance, releasing either the first half of a credit card number or the second would not allow somebody to charge the card. But releasing both would—a composition effect that does not fit into the earlier mould. While this example is extremely simplistic, popular approaches to preserving privacy are vulnerable to similar composition effects both in theory and in practice. 16 In many well-known re-identification attacks—including on the Netflix and AOL datasets and Massachusetts medical records—purportedly anonymised data was sufficiently rich to link to outside public sources of information. While these can be thought of within the framework of composition effects and accumulated privacy risk, they should*

⁵⁸ Jasserand, C. (2016). Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data. Eur. Data Prot. L. Rev., 2, 297.

⁵⁹ Working Party 29, Opinion 4/2007 on the concept of personal data, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

⁶⁰ van der Sloot, B. (2020). *The general data protection regulation in plain language*. Amsterdam University Press.

*not be taken as representative. Composition effects describe a more universal phenomenon: the degradation of privacy protection resulting from multiple uses of data, even if each use is intended to respect privacy.*⁶¹

Thus, it could be argued that even when a health insurer or law enforcement authority will not be able to derive any personal data from specific analysis of sewage material such may yield identifiable information. This may be the case either when they perform structural sewage monitoring activities and are able to connect the various dots, or when they are able to combine data obtained through data analysis of wastewater with other data. Again, whether this is so should be determined on a case-by-case basis, but a very basic example may be the following. In a neighbourhood, law enforcement authorities can see that once a week on a Saturday morning, 3AM, residual material that points to drug consumption is flushed down the sewer. The neighbourhood is a quiet one, primarily inhabited by elderly people, except for one house located at an isolated spot. This house is inhabited by three men that are known to be unemployed, live of social welfare, but drive expensive cars. Such will probably not be enough for the police to act upon, but when two or three other data dots also point in the same direction, such may be enough to treat the sewage data as reliable personal data.

4. Applicability of the right to privacy

The previous section suggested that, apart from the scenario in which the smart toilet is used by one individual or several clearly identifiable individuals, there are many difficult questions about the extent to which the data protection regime applies. Among others, it is uncertain to what extent bodily material itself will be considered personal data. It is uncertain to what extent an anal print is a unique identifier similar to a fingerprint and it will not always be clear how the data protection regime would apply when multiple persons use one toilet. Such depends, inter alia, on what is considered personal data exactly, whether there are additional data available to identify a person and whether the information acquired through data analysis is used as actionable knowledge.

Even if the data protection regime would not apply, the right to privacy might. The right to privacy, as protected by Article 8 of the European Convention on Human Rights, provides protection to bodily integrity, home life and secrecy of correspondence. Paragraph 1 of that provision states that: *'Everyone has the right to respect for his private and family life, his home and his correspondence.'*⁶² This section will show that, similar to the right to data protection, the various use cases of sewage monitoring raise a number of questions with respect to the material scope of the right to privacy.

First, the right to the protection of one's home life, in principle, is a very broad right. The Court has stressed, inter alia, that if a person sleeps either permanently or temporarily in an unconventional home, such as a car, such may be considered a 'home' for the purposes

⁶¹ Fluit, A., Cohen, A., Altman, M., Nissim, K., Viljoen, S., & Wood, A. (2019). Data Protection's Composition Problem. *Eur. Data Prot. L. Rev.*, 5, 285.

⁶² Article 8 European Convention on Human Rights.

of the Convention.⁶³ The Court has made clear that the property need not be owned to be considered a home, for example if a person leases a flat. Neither needs the building be legally occupied. Even when the building was leased by a partner and that partner dies, the surviving spouse may claim that the building as their home. Caravans, second homes, bungalows, and holiday homes may, under circumstances, be considered a home. Even a company's office can be a 'home',⁶⁴ which also holds true for public buildings such as restaurants.⁶⁵ In such cases, the owner of the restaurant can claim that the restaurant is their 'home'. Consequently, the concept of 'home' is so broad that the Court made clear that only buildings such as piggeries will not fall under it.⁶⁶ In addition, when fumes, rays, light, noise, or smog, enter the building, such may be considered an interference with a person's right to privacy.⁶⁷

Consequently, it could be argued that a 'home', in the interpretation by the European Court of Human Rights, is a very broad and all-encompassing concept. Yet, the linking pin to classifying the various facilities, and thereby providing them protection under Article 8 ECHR, is the personal tie an individual has with that building. Such a personal tie may exist either because part of her private life is effectuated there or because such a facility is central to other important aspects of her life, like as a professional working environment. A smart toilet inside the home used for processing personal data would fall under home life. Yet, it is highly unlikely that the same would be the case when robots monitor the sewage right under a person's home, let alone when such is done further down the pipeline by a wastewater facility.⁶⁸ The sewage is not traditionally seen as a place where important and intimate aspects of a person's life are executed, though it cannot be excluded that the ECtHR would treat the sewage as part of the home. If it would, however, the question would arise to what extent, and to what point, the sewage should be considered a part of a person's home and home life: 1 meter down the central sewage pipe, 10 meters, 100 meters?

Second, excrement flushed down the sewage could be likened to garbage put outside the home.⁶⁹ Both excrement and garbage are waste products a person wants to dispose of,

⁶³ ECtHR, McKay-Kopecka v. Poland, appl. no. 45320/99, 19 September 2006. ECtHR, McGonnell v. UK, appl. no. 28488/95, 8 February 2000. ECtHR, Lay v. UK, appl. no. 13341/87, 14 July 1988. ECmHR, Smith v. UK, appl. no. 14455/88, 4 September 1991. ECmHR, Smith v. UK, appl. no. 18401/91, 6 May 1993.

⁶⁴ ECtHR, Stes Colas Est a.o. v. France, appl. no. 37971/97, 16 April 2002.

⁶⁵ <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>.

⁶⁶ ECtHR, Eveau and Fillon v. France, appl. nos. 63512/00 and 63513/00, 06 September 2005.

⁶⁷ ECtHR, Luginbuhl v. Switzerland, appl. no. 42756/02, 17 January 2006. ECtHR, López Ostra v. Spain, appl. no. 16798/90, 9 December 1994. ECtHR, Ledyayeva, Dobrokhotova, Zolotareva and Romashina v. Russia, appl. nos. 53157/99, 53247/99, 56850/00 and 53695/00, 26 October 2006.

⁶⁸ Nield, S. (2013). Article 8 respect for the home: a human property right?. *King's Law Journal*, 24(2), 147-171. Jackson, A. (2018). Home, Human Rights and Horizontal Effect: An English Approach to Article 8 of the European Convention on Human Rights. *Queen Mary Human Rights Review*, 4(1).

⁶⁹ Jennison, W. (1992). Privacy in the Can: State v. Boland and the Right to Privacy in Garbage. *Gonz. L. Rev.*, 28, 159. Piccoli, G. B., Jeantet, A., Gai, M., Burdese, M., Mezza, E., Segoloni, G. P., & Piccoli, G. (2005). Home dialysis, garbage, and privacy: nothing is trivial in home hemodialysis. *Kidney international*, 67(3), 1190.

though they may also reveal a great deal about a person's private life. No jurisprudence is available by the European Court of Human Rights on this point. What is clear though, is that, other Courts have been hesitant to conclude that garbage falls under the protective scope of the right to privacy, especially when put in public waste bins or left outside for the garbage truck to pick up. For example, the American Supreme Court had to issue judgement on the case of a person who was found guilty of third-degree possession of a controlled substance and sentenced accordingly. The police had searched through his garbage and found evidence of methamphetamine. The majority held that a warrantless search of the defendant's garbage was reasonable *'because a person has no reasonable expectation of privacy in garbage set out for collection on the side of a public street because garbage is readily accessible to other members of the public.'*⁷⁰

Still, it could be argued that the difference between searching garbage and sewage monitoring is that the public does not have easy access to the wastewater; rather, to the contrary, it is very difficult to gain access to the sewage. In addition, while no special technological expertise is required to open a bag of garbage and to see what is in it, analysing excrement and other material contained in wastewater requires cutting-edge technology. Usually, only wastewater facilities, law enforcement agencies, and the owners, or operators, of the sewage system have access to the sewage. In addition, while it is well known that garbage can be searched, the general public is mostly unaware of the potential of sewage monitoring. Hence, it could be argued that citizens still have a reasonable expectation of privacy when they go to the toilet.

It could be argued that analysing bodily material could fall under the protection of bodily integrity, also part of the realm of Article 8 ECHR. There are three closely related points in this respect that are worth addressing: whether the processing of data that can be extracted from the faeces should be considered an interference with the right to privacy (third point), whether analysing faeces could be likened to body (cavity) searches (fourth point) and whether the faeces as such could be considered to fall under the material scope of the right to privacy (fifth point).

Third, the right to privacy provides protection to individuals with respect to all kinds of aspects relating to a person's bodily and psychological integrity. This applies to compulsory tuberculin tests or chest x-rays,⁷¹ mandatory vaccination schemes,⁷² gynaecological examinations,⁷³ medical treatments,⁷⁴ and being forced to share an environment where smoking is allowed.⁷⁵ Other examples include disciplinary measures, and punishments

⁷⁰ Campbell, B. (2016). The big stink about garbage: State v. McMurray and a reasonable expectation of privacy. BCJL & Soc. Just., 36, 14.

⁷¹ ECmHR, Acmanne a.o. v. Belgium, appl. no. 10435/83, 10 December 1984.

⁷² ECmHR, Association of parents v. UK, appl. no. 7154/75, 12 July 1978. ECmHR, Wain v. UK, appl. no. 10787/84, 02 December 1985. ECmHR, X. v. Denmark, appl. no. 6907/75, 10 December 1975. ECmHR, Godfrey v. UK, appl. no. 8542/79, 04 February 1982. ECtHR, Storck v. Germany, appl. no. 61603/00, 16 June 2005.

⁷³ ECtHR, Y.F. v. Turkey. appl. no. 24209/94, 22 July 2003. ECtHR, Tomasi v. France, appl. no. 12850/87, 27 August 1992.

⁷⁴ ECmHR, X. v. Germany, appl. no. 8509/79, 05 May 1981.

⁷⁵ ECtHR, Benito v. Spain, appl. no. 36150/03, 13 November 2006.

inflicted by a school,⁷⁶ psychiatric examination ordered by a Court,⁷⁷ the requirement that a prisoner produce a urine sample⁷⁸ and a compulsory medical intervention, even if it is of minor importance.⁷⁹ Bodily and psychological integrity may even extend to the right to euthanasia,⁸⁰ the right to abortion,⁸¹ the positive obligation of the state to ensure access to public buildings for the handicapped⁸² and providing financial assistants for medical treatment.⁸³ Tangentially, the Court has adopted a wide understanding of what falls under the scope of the right to privacy. In part, this is due to the fact that in medical and health related cases, the Court has stressed that *'the notions of personal autonomy and quality of life underpin the right to privacy'*,⁸⁴ as well as a broader notion of 'human dignity'.⁸⁵ Accepting that these values underpin the right to bodily and psychological integrity has allowed the Court to grant the right to privacy a very broad scope, including the processing biometric data and aspects relating to a person's body. For example, the ECtHR provides protection to processing facial images; in *'these cases, the registration and use of facial images have been linked with the right to identity and autonomy'*.⁸⁶ The same applies to, inter alia, being obliged to wear certain clothing or have a certain hair style at work or in prison.⁸⁷

But it is questionable whether analysing excrement would be considered to undermine a person's dignity, autonomy, or identity. It is difficult to lay a direct link between a person's sense of self and their faeces. The Court usually reserves matters of identity to cases in which a person is limited in being themselves or exploring their identity, though that does not seem to be the case in most matters of sewage surveillance. In addition, a person's dignity can be interfered with, the Court has found, when they are subjected to degrading, shameful, or otherwise humiliating treatment. Yet, this will presumably not be the case with most matters of sewage surveillance. Finally, what the Court often finds of particular

⁷⁶ ECtHR, *Costello-Roberts v. UK*, appl. no. 13134/87, 25 March 1993.

⁷⁷ ECmHR, *X. v. Germany*, appl. no. 8334/78, 07 May 1981.

⁷⁸ ECmHR, *A.B. v. Switzerland*, appl. no. 20872/92, 22 February 1995. ECmHR, *Galloway v. UK*, appl. no. 34199/96, 09 September 1998.

⁷⁹ ECmHR, *Peters v. Netherlands*, appl. no. 21132/93, 06 April 1994. ECmHR, *X. v. Netherlands*, appl. no. 8239/78, 04 December 1978. ECmHR, *X. v. Austria*, appl. no. 8278/78, 13 December 1979.

⁸⁰ ECtHR, *Pretty v. UK*, appl. no. 2346/02, 29 April 2002. Sanderson, M. A. (2002). 'Pretty v. the United Kingdom. App. No. 2346/02', Vol. 96 *The American Journal of International Law* No. 4.

⁸¹ ECmHR, *Brüggemann and Scheuten v. Germany*, appl. no. 6959/75, 19 May 1976. ECtHR, *R.R. v. Poland*, appl. no. 27617/04, 26 May 2011. See further: Ireland, E. J. (2013). 'Do Not Abort the Mission: An Analysis of the European Court of Human Rights Case of *R.R. v. Poland*', 38 *North Carolina Journal of International Law & Commercial Regulation* 651.

⁸² ECtHR, *Zehnalova and Zehnal v. Czech Republic*, appl. no. 38621/97, 14 May 2002.

⁸³ ECtHR, *Pentiacova and 48 others v. Moldova*, appl. no. 14462/03, 4 January 2005.

⁸⁴ Van der Sloot, B. (2014). Privacy as human flourishing: could a shift towards virtue ethics strengthen privacy protection in the age of Big Data. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 5, 230.

⁸⁵ Donnelly, M. (2008). From autonomy to dignity: treatment for mental disorders and the focus for patient rights. *Law Context: A Socio-Legal J.*, 26, 37.

⁸⁶ Kindt, E. J. (2013). Biometric data, data protection and the right to privacy. In *Privacy and Data Protection Issues of Biometric Applications* (pp. 87-272). Springer, Dordrecht.

⁸⁷ See inter alia: ECtHR, *Popa v. Romania*, appl. no. 4233/09, 18 June 2013. ECtHR, *Yankov v. Bulgaria*, appl. no. 39084/97, 11 December 2003.

importance in matters concerning individual autonomy is that the body is entered in order to extract material. *The taking of a blood and saliva sample from the applicant constitutes a compulsory medical intervention which, even if it is of minor importance, must consequently be considered as an interference with his right to privacy.*⁸⁸ Finally, what is important to the Court is that such interventions are compulsory. For example, it does not find that voluntary vaccination schemes harm a person's privacy.⁸⁹ Each of these three requirements are not fulfilled by sewage monitoring. Faeces are not considered deeply linked to a person's sense of self nor to her identity. The body does not need to be entered to extract the material, rather it has already left the body, whereby there is no compulsion to use the toilet, though it may of course be argued that citizens do not have a realistic choice to avoid using it.

Fourth, building on the previous point, sewage monitoring could be likened to a body (cavity) search, in particular, when the police use sewage monitoring for criminal law purposes.⁹⁰ Under modern interpretations of the law, body (cavity) searches do not only include physical intrusions by law enforcement officials, but also other ways of extracting information about a person's body. The ECtHR, as discussed above, has indeed suggested that x-rays and other visual forms of bodily intrusion may fall under the material scope of Article 8 ECHR.⁹¹ However, because the faeces have already left the body, no physical, visual, or other intrusions, are required for sewage monitoring. Hence, it is questionable to what extent Courts would liken the analysis of stool and the potential information about a person's body or physical make-up that can be extracted from that as an interference with a person's body.

Fifth, and closely connected to the previous two points, stool could be likened to other bodily material. On the one hand, material such as hair or nails after they have been cut at a barbershop or pedicure are usually legally qualified as residual material and considered a *res nullius*. This is, material with no personal, economic or societal value, over which the former owner no longer holds sway.⁹² On the other hand, it might be argued that in certain jurisdictions, people still have certain rights over limbs or other parts of their body that have been detached from their body, such as after an accident or a medical procedure.⁹³ For example, when finger or hand was torn off during a car crash, the former owner might reclaim ownership over that bodily part to prevent it from being locked, sealed, destroyed,

⁸⁸ ECtHR, *Schmidt v. Germany*, appl. no. 32352/02, 05 January 2006.

⁸⁹ ECtHR, *Baytiire v. Turkey*, appl.no. 3270/09, 12 March 2013.

⁹⁰ La Vigne, N., Lachman, P., Matthews, A., & Neusteter, S. R. (2012). Key Issues in the Police Use of Pedestrian Stops and Searches. *Washington, DC: Urban Institute*. Rogers, M. G. (1986). Bodily Intrusion in Search of Evidence: A Study in Fourth Amendment Decisionmaking. *Ind. LJ*, 62, 1181.

⁹¹ This approach is also adopted by the US Supreme Court: Simonitsch, W. J. (1999). Visual Body Cavity Searches Incident to Arrest: Validity Under the Fourth Amendment. *U. Miami L. Rev.*, 54, 665. Gauthier, C. E. (2011). Is It Really That Simple: Circuits Split over Reasonable Suspicion Requirement for Visual Body-Cavity Searches of Arrestees. *Tul. L. Rev.*, 86, 247.

⁹² See further: Tallacchini, M. (2015). A participatory space beyond the "autonomy versus property" dichotomy. In *Ethics, Law and Governance of Biobanking* (pp. 21-38). Springer, Dordrecht.

⁹³ Gold, E. R. (1996). *Body parts: Property rights and the ownership of human biological materials*. Georgetown University Press.

or used for scientific purposes. At the same time, it seems unlikely that a Court would find that the emotional attachment of a person to her stool is similar to that of a hand or a leg. Subsequently, the European Court of Human Rights has accepted that two forms of surveillance can fall under the scope of Article 8 ECHR: targeted surveillance (the sixth point below) and untargeted surveillance (the seventh point below).

Sixth, targeted surveillance is recognised by the Court. For example, where the telephone or internet communications of a specific person or group is monitored by law enforcement authorities because they are suspected of engaging or having engaged in unlawful conduct. Similar forms of surveillance take place in the sewage, such as when the police has indications that drugs may be produced at a certain building or home, whereby a robot is placed under that home to analyse wastewater. Consequently, although there are similarities, it is still clear that there is one big difference: traditional targeted surveillance falls under the material scope of the right to privacy because Article 8 ECHR provides protection to the privacy of correspondence. The Court has reserved the notion of correspondence for interhuman communication via post, telephone, e-mail, internet, or digital devices. Consequently, it must be assumed that targeted sewage surveillance cannot fall under this aspect of the right to privacy, until the ECtHR determines otherwise.

Seventh, the Court has also accepted another form of surveillance may fall under the scope of Article 8 ECHR, namely untargeted surveillance and the collection of metadata. This typically involves the communications data of large groups or the population as a whole that are harvested to find signals of potential criminal activities or terrorist cells. The ECtHR has accepted that mass surveillance and bulk interception of metadata falls under the scope of Article 8 ECHR, even although collecting and analysing metadata does not violate the privacy of correspondence directly (as these data do not concern the content of communication). This is so because it can give a detailed picture of a person's life. The Court has stressed, among other items, that it is *'not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content.'*⁹⁴ It also stressed, inter alia, that the related communications data *'could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with.'*⁹⁴

On the one hand, it could be argued that mass surveillance is similar to the use case of sewage monitoring in which robots are deployed by law enforcement authorities to float through the sewage system and to constantly monitor wastewater on the presence of prohibited substances. On the other hand, there are clear differences between untargeted sewage surveillance and untargeted interception of communications data. For example, with bulk interception of metadata, intelligence agencies and law enforcement authorities are able to connect the datapoints to specific individuals and to distil patterns of their communications and behaviour from that data. For example, a person phones to Yemen 5

⁹⁴ ECtHR, *Big Brother Watch and Others v. The United Kingdom*, application nos. 58170/13, 62322/14 and 24960/15, 13 September 2018, § 356.

times a day, visits conservative religious websites, and joins internet fora on which persons with a terrorist past are active. The technology to conduct untargeted sewage monitoring is, so far, not that precise. To be similarly precise, the police would, for example, need to monitor all sewage water of a city for a whole month, not just to measure levels of certain substances in general, but on the level of individual faeces. It would need to assess each faecal input and would need to distil patterns (e.g., concerning diet, health, drug use, etc.) on a personal level. This, however, is not the case so far, though it is not excluded that in time, such extensive surveillance technologies would be introduced.

Eighth, the ECtHR has stressed that a chilling effect may constitute an interference with the right to privacy.⁹⁵ For a chilling effect to exist, there need not be a real intrusion (either physical or non-physical): the threat or possibility thereof may be enough. A good example may be the case of *Colon v. the Netherlands*.⁹⁶ In this case, the applicant complained that the designation of a security risk area by the Burgomaster of Amsterdam violated his right to respect for privacy as it enabled a public prosecutor to conduct random searches of people over an extensive period in a large area without this mandate being subject to any judicial review. The government, to the contrary, argued that the designation of a security risk area or the issuing of a stop-and-search order had not in itself constituted an interference with the applicant's private life or liberty of movement. Since the event complained of, several preventive search operations had been conducted and in none of them had the applicant been subjected to further attempts to search him. This was, according to the government, enough to show that the likelihood of an interference with the applicant's rights was so minimal that this deprived him of the status of victim. The Court stressed: *'In principle, it is not sufficient for individual applicants to claim that the mere existence of the legislation violates their rights under the Convention; it is necessary that the law should have been applied to their detriment. Nevertheless, Article 34 entitles individuals to contend that legislation violates their rights by itself, in the absence of an individual measure of implementation, if they run the risk of being directly affected by it; that is, if they are required either to modify their conduct or risk being prosecuted, or if they are members of a class of people who risk being directly affected by the legislation.'*⁹⁷

It went on to explain that it was *'not disposed to doubt that the applicant was engaged in lawful pursuits for which he might reasonably wish to visit the part of Amsterdam city centre designated as a security risk area. This made him liable to be subjected to search orders should these happen to coincide with his visits there. The events of 19 February 2004, followed by the criminal prosecution occasioned by the applicant's refusal to submit to a search, leave no room for doubt on this point. It follows that the applicant can claim to be a "victim" within the meaning of Article 34 of the Convention and the Government's alternative preliminary objection must be rejected also.'*⁹⁸ The applicant was left only the choice between two evils: either he avoided traveling to the capital city of the Netherlands

⁹⁵ 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.

⁹⁶ ECtHR, *Colon v. the Netherlands*, appl. no. 49458/06, 15 May 2012.

⁹⁷ *Ibid.* § 60.

⁹⁸ *Ibid.* § 61.

or he risked being subjected to surveillance activities. This was enough for the Court to accept a victim-status, which it has reaffirmed in later jurisprudence.⁹⁹

The analogy to sewage monitoring is obvious. If people are aware that in their neighbourhood or city, sewage monitoring will be applied, they may be mindful about what they flush down the drain.¹⁰⁰ When their sewage is, or might be monitored, they are faced with a choice: either they subject to monitoring or they avoid using the sewage or use obfuscation techniques, for example buying chemical toilets.¹⁰¹ However, the case is different in that there is hardly a choice not to use the toilet, while there is a realistic choice not to go to the capital of Amsterdam. Whether, consequently, citizens would really avoid using the toilet when aware of the possibility that their stool could be monitored is unsure. Rather, it seems likely that they would buy chemical toilets or use other ways to blur the data obtained through sewage analysis.

Ninth, it could be argued that although sewage monitoring cannot be brought under one of the classic aspects of the legal right to privacy, people also have privacy in public spaces. Under American law, people cannot generally rely on privacy in public spaces and only have marginal 'expectation of privacy'.¹⁰² Still, even in the US, there are cases in which Courts make exceptions¹⁰³ and in literature, it is sometimes argued that when data collection in the public domain is of a systematic and structural nature, such may amount to a privacy violation. *'The mosaic theory of the Fourth Amendment holds that, when it comes to people's reasonable expectations of privacy, the whole is greater than the sum of its parts. More precisely, it suggests that the government can learn more from a given slice of information if it can put that information in the context of a broader pattern, a mosaic.'*¹⁰⁴

In Europe, courts have generally made clear that people also enjoy a right to privacy in the public domain. This even concerns celebrities and royalty. For example, Caroline Von Hannover, the princess of Monaco, had spent more than ten years in unsuccessful litigation in German courts. She alleged that as soon as she left her house, she was constantly hounded by paparazzi who followed her every daily movement, be it crossing the road,

⁹⁹ ECtHR, *Ucar and others v. Turkey*, appl. no. 4692/09, 24 June 2014.

¹⁰⁰ Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Tech. LJ*, 31, 117.

¹⁰¹ Hermstrüwer, Y., & Dickert, S. (2017). Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge. *International Review of Law and Economics*, 51, 38-49.

¹⁰² Shaff, Colin. "Is the Court Allergic to Katz-Problems Posed By New Methods of Electronic Surveillance to the Reasonable-Expectation-of-Privacy Test." *S. Cal. Interdisc. LJ* 23 (2014): 409. Shelton, Alicia. "A Reasonable Expectation of Privacy Online: Do Not Track Legislation." *U. Balt. LJ* 45 (2014): 35. Plourde-Cole, Haley. "Back to Katz: Reasonable Expectation of Privacy in the Facebook Age." *Fordham Urb. LJ* 38 (2010): 571. Roth, David C. "Florida v. Jardines: Trespassing on the Reasonable Expectation of Privacy." *Denv. UL Rev.* 91 (2013): 551. Arrington, Samantha. "Expansion of the Katz Reasonable Expectation of Privacy Test Is Necessary to Perpetuate a Majoritarian View of the Reasonable Expectation of Privacy in Electronic Communications to Third Parties." *U. Det. Mercy L. Rev.* 90 (2012): 179.

¹⁰³ See in particular: *Riley v. California*, 573 U.S. 373 (2014).

¹⁰⁴ Kugler, M. B., & Strahilevitz, L. J. (2016). Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory. *The Supreme Court Review*, 2015(1), 205-263.

fetching her children from school, doing her shopping, going out walking, engaging in sport, or going on holiday. Accepting that there had been an inference with the applicant's private life, the European Court of Human Rights assessed whether the domestic courts had struck a fair balance between the applicant's right to privacy and the press' right to freedom of speech. It considered that anyone, even if they are known to the general public, must be able to enjoy a 'legitimate expectation' of privacy. Increased vigilance in protecting private life, it stressed, is necessary to contend with new communication technologies which make it possible to store and reproduce personal data, adding that *'the distinction drawn between figures of contemporary society "par excellence" and "relatively" public figures has to be clear and obvious so that, in a State governed by the rule of law, the individual has precise indications as to the behaviour he or she should adopt. Above all, they need to know exactly when and where they are in a protected sphere or, on the contrary, in a sphere in which they must expect interference from others, especially the tabloid press.'*¹⁰⁵

In addition, people may even have a reasonable expectation of privacy when they have themselves disclosed private information. For example, in *Pay v. UK* (2008), in which the applicant had joined the Lancashire Probation Service and was involved in the treatment of sex offenders. He was also the director of Roissy, an organisation that advertised its services on the internet as the builder and supplier of BDSM products and the organiser of BDSM events and performances. A photograph of the applicant, wearing a mask, with two semi-naked women was also circulated. Roissy was registered at the applicant's address and its website included links to a number of BDSM websites which advertised various events and included photographs of the applicant and others, semi-naked, performing acts which the accompanying text indicated had taken place at a local private members' club and involved male domination over submissive women. He was fired from work because his behaviour was seen as incompatible with his treatment of sex offenders. The ECtHR acknowledged that the nature of the applicant's acts was shown in the internet photographs and referred to in advertisement. It acknowledged that the applicants conduct and openness about it *'could give rise to doubts as to whether the applicant's activities may be said to fall with the scope of private life and, if so, whether [] there has been a waiver or forfeiture of the rights guaranteed by Article 8. The Court notes, however, that the applicant's performances took place in a nightclub which was likely to be frequented only by a self-selecting group of like-minded people and that the photographs of his act which were published on the internet were anonymised'*.¹⁰⁶

That is why the ECtHR was prepared to assess the case on the assumption that the applicant had a reasonable expectation of privacy and could rely on his rights provided by Article 8 ECHR. Consequently, even if people 'give up' their privacy over their stool by voluntarily disposing of it and flushing it down a public sewage system, it can be argued that they do not intend that material or data derived from it to be disclosed to a broad audience – but at most to the sewage system operator or water management facility - so that they may invoke a right to privacy under Article 8 of the European Convention on Human Rights. However, this analogy would depend on the possibility of sewage system

¹⁰⁵ ECtHR, *Von Hannover v. Germany*, application no. 59320/00, 24 June 2004, § 69

¹⁰⁶ ECtHR, *Pay v. United Kingdom*, application no. 32792/05, 16 September 2008.

operators, law enforcement authorities or other organisations to link back the data derived from sewage monitoring to a specific individual or household.

Finally, even if sewage monitoring would not fall under either of the concepts linked to the right to privacy, if it not considered analogous to mass surveillance and cannot be likened to the reasonable expectation of privacy people have in the public domain. Still, when decisions are made upon the data derived from sewage monitoring that impact a person's private life, such would be considered to fall under the scope for Article 8 of the European Convention on Human Rights. For example, when a health insurer would decide, on the basis of sewage monitoring, no longer to issue insurances in a specific neighbourhood, such might have an impact on the private life of the persons living there. However, whether such a decision would or would not fall under the scope of Article 8 ECHR cannot be established in general, if only because acting upon general statistical information on a population level will generally not be treated as having an impact on a person's right to privacy. This determination will generally depend on two factors: (1) the impact a decision has on a person's freedom, personality or autonomy (the more impact a decision has on these aspects, the sooner it will be linked to a person's right to privacy) and (2) the size of the group covered by the data (the smaller the group, the sooner a decision will be linked to a person's privacy).

5. Legitimacy

It is impossible to discuss the various use cases of sewage monitoring in detail because many of them are still developing. Instead, this section will briefly touch upon a handful of legal questions that sewage monitoring would raise when either the right to data protection, the right to privacy, or both, would apply.

First, if the data protection regime applies, one of the basic requirements would be the 'necessity' requirement,¹⁰⁷ which entails, inter alia, that a technique is effective in light of the goal that is pursued.¹⁰⁸ If ineffective, it would not be necessary to process personal data for that goal. There are many questions regarding the exactitude of sewage monitoring, such as individual recognition via either faeces or anal prints and the feasibility of sewage monitoring for law enforcement purposes. For example, investigatory journalists from several European countries joined in a project¹⁰⁹ analysing how EU-research budgets were spent, and one funded project was assigned to develop a robot for sewage monitoring: Micromole. The article was critical about the results of these funded research projects and in particular zoomed in to the case of sewage monitoring.

'One of those technologies was called MicroMole, developed at a cost of 5.4 million euros by the Fraunhofer Institute for Integrated Circuits (IIS). The technology involved sensors for wastewater pipes to detect if a drug laboratory was in operation in a certain apartment or

¹⁰⁷ See inter alia Article 5 § 1 sub c, d and e GDPR.

¹⁰⁸ Búrca, G. (2000). Proportionality and Subsidiarity as General Principles of Law. In General principles of European Community law (pp. 95-112). Kluwer Academic Publishers. Christoffersen, J. (2009). Fair balance: proportionality, subsidiarity and primarity in the European Convention on Human Rights. Brill.

¹⁰⁹ <<https://thecorrespondent.com/10221/security-for-sale-the-price-we-pay-to-protect-europeans>>.

*home. Ring-shaped devices were to analyze the wastewater in the search for amphetamines and then transmit the data back to headquarters. But to wire a single town such that halfway reliable data could be produced, tens of thousands of the sensors would have been needed, installed at each joint in the sewage system. And even if the enormous effort had been undertaken to assemble the necessary sensors and install them on the pipes buried beneath the city streets, results would have been inexact. Judges would hardly have been likely to issue search warrants for an entire block on the basis of such weak evidence. MicroMole is just one of countless projects that devoured huge sums of money and produced meager results.*¹¹⁰ If technology is that ineffective, gathering large amounts of data about citizens will not pass the test of necessity and proportionality, or that of subsidiarity, as deploying other investigatory tools would be more effective.¹¹¹

Second, the data protection regime underlies the purpose limitation principle.¹¹² The potential of sewage monitoring is both its strength and its weakness, namely that from wastewater and excrement, a wealth of information can be extracted, such as nutrient diet, medicine intake, drug use or production, and the prevalence of diseases, etc.¹¹³ If an insurer covers the costs for a smart toilet in order to advise a patient suffering from diabetes type 2 on diet, exercise, and medicine use, but finds that that patient is also highly likely to produce drugs, it is unclear whether the obligations relating to medical confidentiality prevent it from informing law enforcement authorities.¹¹⁴ Paradoxically, ethical questions might arise when the police are conducting sewage surveillance under a specific home, and finds that a person may be suffering from early stage cancer: should the police have the obligation to inform the person of such fact, even if that means aborting secret surveillance activities?¹¹⁵

Third, if smart toilets are able to perform analysis on an individual level, either on the basis of faecal input, anal prints, or additional means of identification, such as camera's hanging outside a restroom, the question of legitimate grounds for processing personal data arises.¹¹⁶ For smart toilets placed inside a person's home, the people living there might give informed consent. But such would already be substantially more difficult when they have

¹¹⁰ <<https://www.zeit.de/wirtschaft/2017-02/security-technologies-eu-terror-research-fraunhofer/seite-2>>.

¹¹¹ Shaw, K. (2018). The Court of Justice of the European Union: Subsidiary and Proportionality. Brill.

¹¹² Article 5 § 1 sub b GDPR.

¹¹³ Brouwer, E. R. (2011). Legality and data protection law: The forgotten purpose of purpose limitation. Forgó, N., Händl, S., & Schütze, B. (2017). The principle of purpose limitation and big data. In New technology, big data and the law (pp. 17-42). Springer, Singapore.

¹¹⁴ Jasserand, C. (2018). Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle Purpose Limitation. Eur. Data Prot. L. Rev., 4, 152.

¹¹⁵ Von Grafenstein, M. (2018). The Principle of Purpose Limitation in Data Protection Laws. Nomos Verlagsgesellschaft mbH & Company KG. Koning, M.E. (2020) The purpose and limitations of purpose limitation <https://merelkoning.nl/wp-content/uploads/2020/10/M.Koning_The-purpose-and-limitations-of-purpose-limitation_thesis.pdf>.

¹¹⁶ Ross, H. (2017). Data subject consent: How will the General Data Protection Regulation affect this?. Journal of Data Protection & Privacy, 1(2), 146-155.

visitors that want to use the toilet.¹¹⁷ Explaining to them in detail what data may be extracted from their excrement, who has access to those data, and under which conditions, might take considerable time.¹¹⁸ Obtaining a legal ground for processing becomes even more difficult when smart toilets are placed in public facilities.¹¹⁹ Just hanging a signpost or general leaflet on the side of the wall does not result in explicit, active, and unambiguous consent, for the purpose of the GDPR.¹²⁰ It is also unlikely that any other of the ground mentioned in Article 9 GDPR would apply to monitoring faeces at an individual level,¹²¹ apart from sewage monitoring of specific suspects by the police. For example, general sewage monitoring on a population level to be used in the fight against the Corona virus, the GDPR would most likely not apply and would thereby provide a ground for processing under the protection of public health.

Fourth, many of the sewage monitoring systems deployed at an individual level allow for automatic decision making.¹²² Potentially, smart toilets can be connected to databases of general practitioners or pharmacists, to make decisions about drug prescription or treatment. Also, health insurers might want to have access to such data and may determine the costs for the insurance based on faecal research, but such items remain hypothetical.¹²³ If they would become real, Article 22 GDPR would apply, paragraph holding: *‘The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.’* However, paragraph 2 stresses that that prohibition will not apply if the decision: *‘(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or (c) is based on the data subject’s explicit consent.’* Furthermore, paragraph 4 stresses that such decisions may even be based on sensitive personal data when the data subject has given explicit consent or when a substantial public interest is at stake. Such an exception may apply when automatic decision making is connected to the use of a smart toilet to which a person has agreed or when a smart toilet in a public facility could detect traces of

¹¹⁷ Whitley, E. A. (2009). Informational privacy, consent and the “control” of personal data. Information security technical report, 14(3), 154-159.

¹¹⁸ Mostert, M., Bredenoord, A. L., Biesaat, M. C., & Van Delden, J. J. (2016). Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. *European Journal of Human Genetics*, 24(7), 956-960.

¹¹⁹ Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent: a patient interface for twenty-first century research networks. *European journal of human genetics*, 23(2), 141-146.

¹²⁰ Parker, L. (2011). Using human tissue: when do we need consent?. *Journal of medical ethics*, 37(12), 759-761.

¹²¹ Voigt, P., & Von dem Bussche, A. (2017). *The eu general data protection regulation (gdpr). A Practical Guide*, 1st Ed., Cham: Springer International Publishing.

¹²² Roig, A. (2017). Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). *European Journal of Law and Technology*, 8(3).

¹²³ Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, 7(2), 76-99.

a virus (e.g., of Covid19) – whereby public health concerns would conceivably warrant action.

Law enforcement agencies already experiment with such systems for automatic decision making. For example, agencies use a robot for untargeted sewage surveillance, where that robot automatically decides to move toward the locus of where a certain substance is discharged in order to gather criminal evidence. Another situation is where law enforcement agencies place a robot under a facility to give the police a sign when the sewage is used to discharge waste from drug production, in order to swiftly raid the building and catch the perpetrators while engaged in criminal activities.¹²⁴ These types of actions have legal consequences and can have a significant impact on a person, but the Law Enforcement Directive¹²⁵ does not prohibit such automated decision making. Rather, it specifies: *'1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller. 2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'*¹²⁶ Consequently, whether such use cases are prohibited depends on the legal regime in place.¹²⁷

Fifth, when untargeted sewage monitoring is likened to untargeted collection of metadata and would consequently be said to fall under the material scope of Article 8 ECHR, it is important that the European Court of Human Rights requires States to lay down detailed regulations.¹²⁸ Elaborate legal regimes exist for the purpose of targeted monitoring of individuals or small groups suspected of criminal activities in most jurisdictions. Usually, a judge or public prosecutor needs to give prior authorisation to law enforcement agencies based on a reasonable suspicion before they can start their monitoring activities. In addition, the person monitored needs to be informed, after the investigations have been finalised, of the fact that she was subject to targeted surveillance measures and about whether or not charges will be pressed. When applying this regime to bulk surveillance,

¹²⁴ Škorvánek, I., Koops, B. J., & Timan, T. (2019). Surveillance, Criminal Procedure, and Regulatory Connection: the Case of Sewage Monitoring. *Tilburg Law School Research Paper Forthcoming*.

¹²⁵ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

¹²⁶ Article 11 Law Enforcement Directive.

¹²⁷ Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, 34(2), 398-404.

¹²⁸ Coleman, R., & McCahill, M. (2010). Surveillance and crime. Sage.

the problem is twofold.¹²⁹ On the one hand, legal regimes are often not designed to cover these forms of surveillance. For example, the very notions of reasonable suspicion and prior authorisation does not apply to untargeted surveillance.¹³⁰ On the other hand, because every citizen or large parts of the population are subjected to bulk interception, they cannot be informed individually. This means that there are neither substantial *ex ante* checks on the use of power nor *ex post* claims by citizens that challenge the legitimacy of these types of measures.¹³¹

That is why the Court has stressed that additional legal safeguards should be implemented in laws authorising untargeted surveillance and to implement detailed rules on at least nine points. (1) Accessibility of the domestic law. (2) Scope of application of secret surveillance measures. (3) The duration of secret surveillance measures. (4) Procedures for processing the data. (5) Authorisation procedures. (6) *Ex post* supervision of the implementation of secret surveillance measures. (7) Conditions for communicating data to and receiving data from other parties. (8) Notification of interception of communications. (9) Available remedies.¹³² This means that when untargeted sewage surveillance would be implemented, either by the police in terms of locating drug producers, or by public facilities using smart toilets in a non-individualizable manner to find facts about drug consumption or health risks of customers or visitors, detailed legal regimes would need to be implemented on at least these nine points.

Finally, when public organisations use sewage surveillance either for combatting crime or for public health reasons, such would need to pass the necessity test. Paragraph 2 of Article 8 European Convention on Human Rights specifies: *‘There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.’* With regard to the ‘accordance with the law’ criterion, such would require a law specifying detailed rules on the nine points previously mentioned. With respect to finding a public interest for sewage monitoring, such would not be a problem, as it would be either in the interest of the public in light of the protection of public safety or the prevention of disorder and crime or for the protection of health. This leaves the necessity test, which is commonly interpreted by the Court as a balancing test. *‘Establishing that the measure is necessary in*

¹²⁹ Decker, C. (2007). Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime. S. Cal. L. Rev., 81, 959.

¹³⁰ Powell, M. A. (2019). CRIMINAL PROCEDURE—Jurisdictional Limitations on Federal Judges’ Ability to Authorize Electronic Surveillance: A Cry for Congressional Guidance. University of Arkansas at Little Rock Law Review, 41(3), 437. Turner, A. (2017). Wiretapping Smart Phones with Rotary-Dial Phones’ Law: How Canada’s Wiretap Law Is in Desperate Need of Updating. Man. LJ, 40, 249.

¹³¹ Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. Ethics and Information Technology, 18(1), 33-39. Henschke, A. (2017). Ethics in an age of surveillance: Personal information and virtual identities. Cambridge University Press.

¹³² ECtHR, Roman Zakharov v. Russia, appl. no. 47143/06, 04 December 2015. ECtHR, Centrum för Rättvisa v. Sweden, appl. no. 35252/08, 19 June 2018. ECtHR, Big Brother Watch and others v. the United Kingdom, appl. nos. 58170/13, 62322/14 and 24960/15, 13 September 2018.

*a democratic society involves showing that the action taken is in response to a pressing social need, and that the interference with the rights protected is no greater than is necessary to address that pressing social need. The latter requirement is referred to as the test of proportionality. This test requires the Court to balance the severity of the restriction placed on the individual against the importance of the public interest.*¹³³

It is obviously impossible to know what the Court would determine on this point vis-à-vis the wide range of potential use cases for sewage monitoring. Two points are important. On the one hand, it could be argued that sewage monitoring is a potentially highly invasive form of surveillance that can result in very detailed and diversified data patterns about individuals or the population at large. Even if not linked to specific individuals, the fact that certain groups, for example immigrants, have a higher prevalence of certain diseases or that in immigrant neighbourhoods, drug consumption is higher, might be used and abused by all kinds of parties. On the other hand, the Court has on many occasions stressed that countries do not only have negative obligations, that is, the obligation to not interfere with the human rights of citizens, unless it is strictly necessary. Governments also have the positive obligation to ensure that the population is safe and healthy.¹³⁴ Given the fact that drug use can do harm to individual health and can lead to domestic violence and that waste material dumped in the sewage or in the environment can lead to environmental harm and higher costs for wastewater treatment. Given that drug production can lead to drug violence of criminal gangs and associated violence, it can be argued that states have positive obligation to conduct sewage monitoring to keep its population safe. The same may be argued for conducting sewage monitoring in order to benefit the health of the general population. For example, if it is known that a significantly higher number of children are suffering from obesity, the government might invest in healthy food programs or in educating more medical professionals that are trained to deal with the consequences of obesity, such as diabetes or heart and vascular diseases.

6. Conclusion

Sewage monitoring is a new form of surveillance that is still in its infant years. It is unclear how the various technologies that are currently being developed will be implemented in practice. Yet, there are several use cases that are currently tested. Among them are the use of smart toilets for medical diagnoses, sewage monitoring for determining the prevalence of diseases and viruses such as Covid19, and the analysis of wastewater from specific homes or areas in order to identify drug production facilities. In addition, smart homes and cities are built that incorporate sewage surveillance as a central element and toilets are introduced that can identify individuals on the basis of their unique anal print. When installed in public buildings, smart toilets could make a wealth of information about individual citizens available to governmental organisations, restaurants and other public facilities.

¹³³ Ovey, C. & White, R.C.A. (2002). 'European Convention on Human Rights', Oxford University Press, Oxford, p. 209.

¹³⁴ Mowbray, A. (2004). The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights. Bloomsbury Publishing.

Although these developments can clearly have a big impact on the individual freedoms of citizens and their rights, it is not a given that either the right to data protection or the right to privacy or both would apply. Apart from the smart toilet being used by one individual or several clearly identifiable individuals, it may be difficult to apply the data protection regime. It is uncertain to what extent bodily material itself should be considered personal data, to what extent an anal print is a unique identifier similar to a fingerprint and there are obstacles to distilling individual patterns from mixed or polluted water. Even if the data protection regime would not apply, however, it could be argued that the broader right to privacy does. However, similar questions arise. Although the concept of 'home' is interpreted broadly by the ECtHR, it is unlikely that the sewage under the home will be considered part of it. In addition, although there are arguments in favour of treating bodily parts as falling under the scope of the right to privacy, there are also arguments against, such as that there is generally no link between a person's excrement and their sense of self and autonomy of dignity. Finally, different from bulk interception of metadata, sewage monitoring is not sufficiently precise to identify individual faecal patterns.

If either of these two regimes would apply, sewage monitoring would raise a number of difficult legal questions. Not all of these questions have been discussed in detail. This is because there are so many legal questions and because many of the use cases are still developing. One issue would definitely be the effectiveness of sewage monitoring activities, for example by law enforcement authorities, about which there are doubts. In addition, the purpose limitation principle could block a number of potentially more *avant garde* applications of sewage surveillance. Apart from explicit consent by residents of a home equipped with a smart toilet and sewage monitoring of specific suspects by the police, it will be difficult to find a legitimate ground for processing personal data. With respect to the right to privacy, the ECtHR would require an elaborate legislative regime for untargeted forms of sewage surveillance, at least on the nine points. (1) Accessibility of the domestic law. (2) Scope of application of secret surveillance measures. (3) The duration of secret surveillance measures. (4) Procedures for processing the data. (5) Authorisation procedures. (6) Ex post supervision of the implementation of secret surveillance measures. (7) Conditions for communicating data to and receiving data from other parties. (8) Notification of interception of communications. (9) Available remedies. Finally, whether the ECtHR would find sewage monitoring necessary in a democratic society would depend on the circumstances of the case. In general, sewage monitoring is a highly invasive technique that can yield unprecedented amounts of detailed and sensitive data. However, it can help the fight against drug production and associated violence and can be used to yield data on public health aspects, such as Covid19 outbreaks.

Whether the current privacy and data protection regimes adequately tackle the issue of sewage monitoring should be carefully scrutinised and debated, both in scholarly literature, in the regulatory context and preferably also by the general public as it raises important questions related to privacy, public health, and law enforcement. Although some use cases seem to fall under the scope of these regimes, others do not, and if they do, only under certain circumstances. It should be assessed whether this is justified or whether additional regulation is necessary to regulate specific use cases currently falling outside the existing legal frameworks. In addition, because sewage monitoring is so

different from most traditional forms of data collection, deployed either for public health or criminal law purposes and because the technique is potentially so invasive, it might be prudent to carefully verify whether the current conditions, checks and balances, to assist in providing a regulatory oversight are sufficient to ensure that sewage monitoring does not become the darkest of all surveillance tools.