

Wolfie Christl

TRACKING INDOOR LOCATION, MOVEMENT AND DESK OCCUPANCY IN THE WORKPLACE

**A case study on technologies for behavioral
monitoring and profiling using motion sensors
and wireless networking infrastructure
inside offices and other facilities**



A CASE STUDY BY CRACKED LABS

Vienna, November 2024

This publication is part of the project "Surveillance and Digital Control at Work": crackedlabs.org/data-at-work

Tracking Indoor Location, Movement and Desk Occupancy in the Workplace

A case study on technologies for behavioral monitoring and profiling using motion sensors and wireless networking infrastructure inside offices and other facilities.

Cracked Labs, November 2024.

Author: Wolfie Christl

Edited by: Mike Holohan

© 2024 Cracked Labs

Every effort has been made to ensure the accuracy of the texts in this report. The author and the publisher accept no liability in the case of eventual errors. Unless indicated otherwise, the contents of this publication are licensed under the terms of CC BY-SA 4.0.

Cracked Labs – Institute for Critical Digital Culture

Gumpendorfer Straße 63b, 1060 Vienna, Austria

<https://crackedlabs.org>

This publication is part of the project “Surveillance and Digital Control at Work”, which aims to explore and examine how companies use personal data on workers in Europe.

<https://crackedlabs.org/data-at-work>

The production of this publication was supported by the “Digitalisierungsfonds 4.0” of AK Wien.

Contents

Summary	4
1. Introduction, background and overview	9
2. Monitoring desk and room occupancy with motion sensors	10
2.1 Spacewell – “workplace analytics” based on motion and presence detection	10
2.1.1 Motion and presence detection.....	11
2.1.2 Sensor hardware based on heat detection, visual analytics and other technologies.....	11
2.1.3 “Space monitoring” and “workplace analytics” for different purposes	12
2.1.4 Room reservations, flexible desking and “smart” cleaning based on sensor data	12
2.1.5 Privacy and data protection considerations.....	13
2.2 Locatee – behavioral profiling based on motion sensor, badge and device location data.....	14
2.2.1 Analyzing employee and team behaviors	14
2.3 Practical examples and worker resistance	15
3. Tracking indoor location, movements and behaviors	17
3.1 Indoor location tracking	17
3.2 Turning Cisco’s network infrastructure into a location tracking system	17
3.2.1 Indoor location tracking via Wi-Fi and BLE technology	18
3.2.2 Behavioral profiling based on location data.....	19
3.2.3 Analyzing movements and behaviors at the individual level	19
3.2.4 Tracking indoor behavior with Cisco’s security cameras and WebEx devices	20
3.2.5 Applications for Cisco’s location tracking system.....	21
3.2.6 Privacy and data protection considerations.....	22
3.2.7 Third-party applications based on Cisco Spaces	23
3.3 Locating nurses, security guards and sales associates with Juniper Networks	23
List of figures	25
References	25

Summary

As offices, buildings and other corporate facilities become networked environments, there is a growing desire among employers to exploit data gathered from their existing digital infrastructure or additional sensors for various purposes. Whether intentionally or as a byproduct, this includes personal data about employees, their movements and behaviors.

Technology vendors are promoting solutions that repurpose an organization's wireless networking infrastructure as a means to monitor and analyze the indoor movements of employees and others within buildings. While GPS technology is too imprecise to track indoor location, Wi-Fi access points that provide internet connectivity for laptops, smartphones, tablets and other networked devices can be used to track the location of these devices. Bluetooth, another wireless technology, can also be used to monitor indoor location. This can involve Wi-Fi access points that track Bluetooth-enabled devices, so-called "beacons" that are installed throughout buildings and Bluetooth-enabled badges carried by employees. In addition, employers can utilize badging systems, security cameras and video conferencing technology installed in meeting rooms for behavioral monitoring, or even environmental sensors that record room temperature, humidity and light intensity. Several technology vendors provide systems that use motion sensors installed under desks or in the ceilings of rooms to track room and desk attendance.

This case study explores software systems and technologies that utilize personal data on employees to monitor room and desk occupancy and track employees' location and movements inside offices and other corporate facilities. It focuses on the potential implications for employees in Europe. To illustrate wider practices, it investigates systems for occupancy monitoring and indoor location tracking offered by Cisco, Juniper, Spacewell, Locatee and other technology vendors, based on an analysis of technical documentation and other publicly available sources. It briefly addresses how workers resisted the installation of motion sensors by their employers. This summary presents an overview of the findings of this case study.

Occupancy monitoring and "workplace analytics" with motion sensors

The Belgian-German vendor **Spacewell** offers a system for "real-time office space monitoring" and "workplace analytics" that monitors and analyzes how employees use desks, meeting rooms, office floors and entire buildings:¹

- Spacewell uses sensors installed under desks, in the ceiling and at doors to track desk attendance and count the number of people in rooms. In addition to motion sensors that detect heat emitted by human beings, the system uses visual sensors that analyze "low-resolution" images of rooms, which represents a form of video surveillance based on computer vision and AI. An example in Spacewell's technical documentation shows an office floor with 75 motion sensors, 16 "headcount" sensors and two "doorcount" sensors installed at restroom doors.
- The system's "live data floorplan" and "space monitor" show which rooms and individual desks in the office are occupied, both in real time and over time. While electronic floorplans that disclose desk presence typically do not display employee names, employees can be identified based on information about their assigned desks. An additional system allows employees to book meeting rooms, or, in cases where flexible seating is used, also desks. The booking system can show where specific named employees are currently seated on the floorplan.

¹ More information about Spacewell's data practices, including sources for quotes and other statements, can be found in section 2.1. Note: The research in this case study refers to products offered by Spacewell in September 2023.

- According to Spacewell, employers can use the system to “get a detailed picture of how the building is used during the day”, “identify underused areas”, “reduce underutilized space”, “save on rent, energy and cleaning” and “optimize workplace experience”. The company explains that employers can “sit back and watch it as a movie” in order to “get a feeling of how presence, utilization, and comfort parameters evolve during the day”. Spacewell provides additional functionality that utilizes sensor data, such as a “smart” cleaning application.
- Room temperature, humidity, light intensity and other environmental sensor data can also be utilized to analyze room occupancy. However, Spacewell states that the accuracy is low in this case.
- While the system offers some functions and information that address data security, employee privacy and data protection, Spacewell does not adequately engage with the risks posed by behavioral monitoring and profiling.

The Swiss vendor **Locatee** offers a “workplace analytics” system that additionally utilizes badge and device data:²

- Locatee explains that while motion sensors “provide the most precise and granular level of data”, the “advantage” of using badge data “is that it relies on technologies which are often already in place”. Wi-Fi and LAN data can also be utilized to monitor occupancy, as it provides “continuous and real-time data on the whereabouts” of devices, according to the company.
- Locatee provides reports on “people behavior metrics” and “people presence enriched with team information”. Employers can analyze how many employees attend the office each day, how many days a week they come in, how many hours they spend there per day, how much time they spend at their desks and at which times they enter and leave the building. While these reports display aggregate numbers, they utilize behavioral profiling based on extensive personal data. The “team analytics” report, which analyzes how many hours particular teams spend in the office and how much time they spend on each floor, reveals data on small groups.

In several cases, employers installing under-desk motion sensors led to **worker protests and media debates**, ultimately leading to their removal:³

- This happened, for example, at the UK newspaper “The Daily Telegraph” and the UK bank Barclays. Both companies installed sensors from OccupEye, a firm that has since been acquired by the facility technology vendor **FM:Systems**, which states that it has deployed 250,000 sensors at 1,200 client sites across 80 countries. FM:Systems published aggregate analyses of office occupancy from employers in the US and EU on its website, which suggests that it exploits sensor data and thus employee data for its own promotional purposes.
- Student workers at the US-based **Northeastern University** also successfully resisted the deployment of motion sensors, considering them to be “intimidating” and “unnecessary” surveillance that serves “no scientific purpose”. The installed sensors came from **EnOcean**, a German vendor whose marketing materials promote the deployment of “presence detection”, “people counter” and “door detection” sensors, even in restrooms.

Tracking indoor location, movement and other employee behavior

The network technology giant **Cisco** offers a product that turns wireless networking infrastructure and other technologies already installed in a building into a system that tracks the location of employees, customers, devices and other objects for a wide range of purposes.⁴ It allows companies to “gain insights into how people and things move

² More information about Locatee’s data practices, including sources for quotes and other statements, can be found in section 2.2

³ See section 2.3

⁴ More information about Cisco’s data practices, including sources for quotes and other statements, can be found in section 3.2

throughout their physical spaces” and “understand the behavior and location of people (visitors, employees) and things (assets, sensors)”. Companies can get a “real time view of the behavior of employees, guests, customers and visitors” and “profile” them based on their indoor movements in order to “get a detailed picture of their behavior”:

- Cisco tracks the location of laptops, smartphones and other devices that connect to its Wi-Fi access points. It can also use other wireless technologies such as Bluetooth/BLE for location tracking. The system processes indoor location data on a massive scale and frequency. An example report shows how monitoring only 138 persons who visited a building via 11 Wi-Fi access points generated several million location records.
- Employers can see the current location of each device in the building on a map, access data on past movements and search for devices in order to locate them. Employees who carry these devices can be identified via pseudonymous device identifiers or usernames. As such, the system processes extensive personal data on employees. A “proximity tracking” application introduced by Cisco during the coronavirus pandemic demonstrates that the system is well equipped to track the movements of named employees at the individual level.
- The system provides aggregate reports that display, for example, the number of persons currently located in a building. In addition, it can categorize people based on their movements and behavioral profiling. It goes far beyond aggregate analysis and makes it possible to identify, single out and target individuals in several ways.

Cisco promotes various applications for its location tracking system that affect both customers and employees:

- Companies can use the system to track, profile and target their customers. Retailers, restaurants, hotels or event venues can identify, for example, loyalty members, weekend visitors, customers who visit certain areas or those who return often. Based on behavioral profiling, they can target them with promotions or personalized recommendations via mobile app. They can also use the data to make decisions about their buildings, the services they offer and about staff and cleaning schedules. Cisco describes many other applications for the system, including indoor navigation at airports, patient tracking in hospitals and student attendance tracking at universities.
- As employers, companies can use the system to track, profile and target employees. They can use it for occupancy monitoring, meeting room management and other applications that turn offices into “smart workplaces”. Employers can access aggregate analyses about employees’ entry and exit times, workday durations, visit durations by floor and other “behavior metrics”. They can profile employees, send them notifications based on their movements and measure the impact of internal campaigns that aim to change their behavior.
- Other applications promoted by Cisco can have even more consequential implications for employees. Employers in manufacturing can use the system to “understand employee behavior that affects performance” and thus for performance monitoring. In the name of workplace safety and security, they can receive alerts when equipment used by employees enters “restricted zones” or leaves the facility. Similarly, retailers can detect “any deviance from usual asset usage”. Employers in various sectors can use the system for behavioral surveillance in cybersecurity that aims to prevent data theft. Hospitals can use it to “automate monitoring and reporting of hand hygiene compliance”. Cisco generally promotes applications for occupational health purposes.

Employers can use Cisco’s cloud-based indoor location tracking system to collect, analyze and utilize extensive personal data on employee movements and other behaviors inside buildings:

- Cisco claims that it has so far processed 17.2 trillion “location data points” collected via 3.1 million Wi-Fi access points installed in 250,000 buildings. It offers employers the ability to compare behavioral metrics with

other organizations and states that it uses client data for its own purposes, including for “understanding product usage and enabling product improvements”. As Cisco is a global core infrastructure vendor, this is concerning.

- By default, the system collects “MAC addresses” that identify employee devices. While it supports “MAC randomization” to “limit user tracking and support privacy requirements”, Cisco emphasizes that this option will render location analytics “unreliable” and make several applications impossible. The company also emphasizes that employers can export location data to “correlate” it “with other data sources” and integrate it with other enterprise software such as “human resource management systems”.
- Third-party vendors can offer applications that are integrated with Cisco’s data. Locatee offers an application that utilizes Cisco’s location tracking data for its workplace analytics system. IBM offers an application that utilizes Cisco data to analyze how employees use offices and desks and how they move in buildings. It also provides “anomaly detection”, promising to detect occupancy patterns that deviate from “normal” patterns.
- In addition to wireless networking infrastructure, the system can also turn Cisco’s security cameras and the company’s WebEx video conferencing devices into sensors. Data from video cameras can be utilized to analyze the “behavior of people within physical spaces”, for example, by tracking the number of persons staying in a space, entering or exiting it. As such, Cisco repurposes data from a highly intrusive video surveillance system, originally intended for security and safety purposes, to analyze indoor movements.

Juniper, another large network technology vendor, offers a similar indoor location tracking system:⁵

- Juniper uses both Wi-Fi and Bluetooth/BLE technology to locate objects, employees and other persons in buildings. Its Wi-Fi access points can locate people either via their devices or via extra badges carried by them. Employers can see the current location of each device in the building on a map and analyze up to 13 months of past data to “perform long-term historical time series analyses” of employee behavior.
- The system provides reports about how employees move between different “zones” in offices and buildings. An example report in Juniper’s technical documentation shows how 551 employee devices were located in a zone labeled “break area / kitchen”, with an average duration of 13.5 minutes per visit. The report also provides records about each tracked activity, including the “device name” and the exact “enter” and “exit” times.
- Juniper promotes various applications for its system. In addition to optimizing “space utilization by tracking employee traffic patterns” in offices, employers can use it to “locate key human resources such as nurses, security guards, and sales associates”. Retailers can use it to “track personnel and equipment”, “optimize shelf management” and prevent theft. Hospitals can use it to monitor “employee health and safety”. Manufacturers can use it “optimize workflows”. Together with third-party vendors, Juniper provides “tailored workflow applications” that utilize its location tracking system and “enable data-driven decision making”.

Concluding remarks

Tracking and analyzing employees’ desk presence, indoor location and movements represents intrusive behavioral monitoring and profiling. Even if employers analyze the data only at the aggregate level, they process extensive personal data on employee behavior. Once deployed in the name of “good”, whether for worker safety, energy efficiency or just improved convenience, these technologies normalize far-reaching digital surveillance, which may quickly creep into other purposes. Whether based on existing infrastructure or newly installed tracking technology,

⁵ More information about Juniper’s data practices, including sources for quotes and other statements, can be found in section 3.3

the systems examined in this case study raise serious concerns about employee privacy and data protection in the workplace.

The findings of this case study will be incorporated in the main report of the ongoing project “Surveillance and Digital Control at Work” (2023-2024) led by Cracked Labs, which aims to explore how companies use personal data on workers in Europe. The main report will draw further conclusions.

1. Introduction, background and overview

This case study explores and examines technologies and software systems that allow employers to monitor room and desk occupancy, indoor location, movements and other employee behaviors inside offices and other corporate facilities. It focuses on the potential implications for employees in Europe and documents data practices by examining software that is available on the market and sold to employers, based on an analysis of publicly available corporate sources such as software documentation, training videos and marketing materials.

To illustrate wider practices, **this case study investigates** how systems for occupancy monitoring and indoor location tracking offered by Cisco, Juniper, Spacewell, Locatee and other vendors process personal data on employees. In addition, it briefly addresses how workers have resisted the installation of motion sensors by their employers.

- **Section 2** explores how employers can monitor and analyze room and desk occupancy based on motion and visual sensors inside offices. It investigates systems for “real-time office space monitoring” and “workplace analytics” offered by the two European technology vendors Spacewell and Locatee. It briefly addresses technologies from other vendors and presents examples of how employers installing under-desk motion sensors led to worker protests, media debates and ultimately to their removal.
- **Section 3** examines an indoor location tracking system provided by the networking technology giant Cisco that utilizes Wi-Fi access points and other technologies to locate employees and other persons inside buildings and analyze their past movements at the individual level. It shows how employers can use the system for behavioral profiling and documents various applications ranging from the aggregate analysis of movement patterns to performance monitoring in manufacturing. Furthermore, it investigates a similar indoor location tracking system provided by the network technology vendor Juniper, which is designed to single out employees at the individual level.
- This initial “summary” section presents an overview of the findings of the investigation.

This case study is part of a series of case studies on systems that process data at the workplace, which are, in turn, part of the **ongoing project**, “Surveillance and Digital Control at Work”,⁶ led by Cracked Labs. The project aims to explore how companies use personal data on and against workers in Europe, together with AlgorithmWatch, Jeremias Prassl (Oxford), UNI Europa and GPA, funded by the Austrian Arbeiterkammer. The case studies build on **previous research** on the topic (Christl, 2021). They aim to document technologies and data practices by reviewing existing literature and by **examining technologies and software systems** that are available on the market based on publicly accessible vendor information. This includes software documentation and marketing materials, which might be ambiguous and incomplete. Every effort has been made to accurately interpret these corporate sources, but we cannot accept any liability in the case of eventual errors. Where the case studies rely on the examination of corporate sources, it remains largely unclear how employers actually implement, customize and use the functionality provided by these systems. The findings of the case studies will be incorporated into the **main report** of the ongoing project, which will draw further conclusions from the findings.

⁶ <https://crackedlabs.org/en/data-at-work>

2. Monitoring desk and room occupancy with motion sensors

Several vendors offer workplace technology that utilizes motion sensors installed under desks, in ceilings and in other places in the office to monitor and analyze desk and room occupancy.

2.1 Spacewell – “workplace analytics” based on motion and presence detection

Spacewell, a Belgian company owned by German Nemetschek Group,⁷ offers⁸ systems for “real-time office space monitoring”⁹ and “workplace analytics”¹⁰ that promise to monitor and analyze the use of desks, meeting rooms, office floors and entire buildings. Data sources can include motion sensors installed under desks¹¹ and other presence detection sensors installed in the ceilings of meeting rooms and collaboration spaces, next to doors, in “transit zones” and in other places in the office.¹²

As figure 1 (left) shows, the system provides insight into **desk occupancy for individual workplaces**, both in real time and over time. The red areas on the map represent desks where employee presence was detected. The green areas represent desks that are currently not occupied.

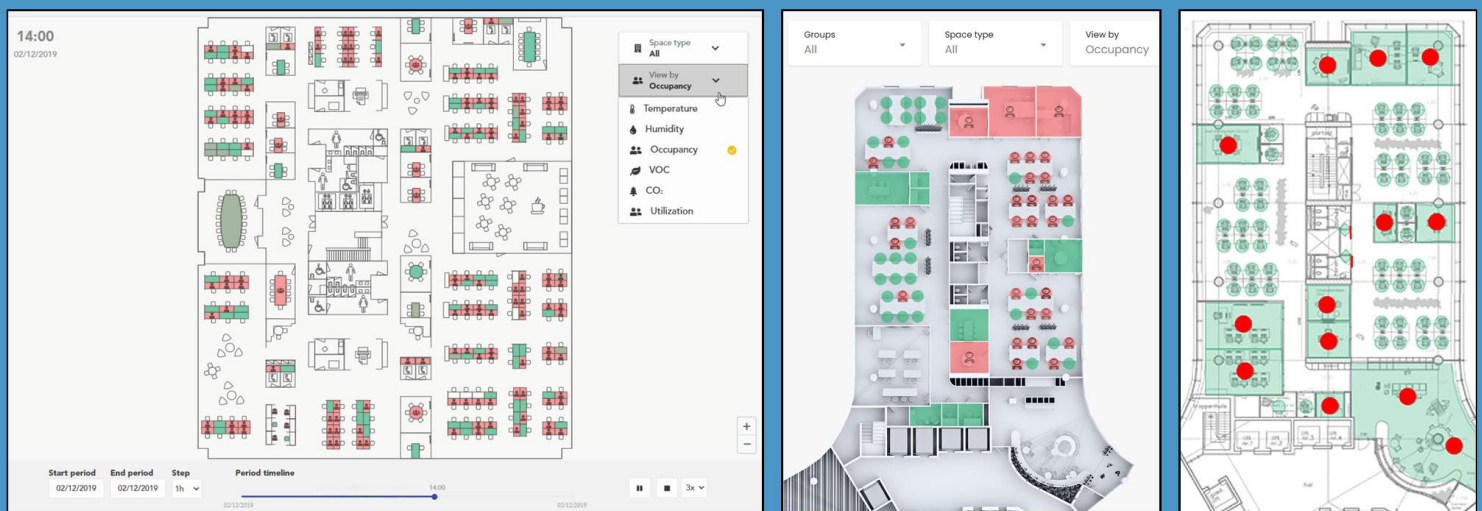


Figure 1: Desk and room occupancy monitoring (Spacewell)¹³

⁷ <https://spacewell.com/company/about-us/>, <https://www.nemetschek.com/en/contact> [27.9.2023]

⁸ This research was carried out in September 2023. As of 2024, Spacewell’s website has changed. The original website, including several subpages cited in this case study, are available on archive.org: <https://web.archive.org/web/20230929112101/https://spacewell.com/>

⁹ <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/space-monitor/> [26.9.2023]

¹⁰ <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/> [28.9.2023]

¹¹ <https://support.spacewell.com/space/KB/5242896/External+Data+Sources>, <https://support.spacewell.com/space/KB/491737>, <https://support.spacewell.com/space/KB/232292388>, video min 0:29: <https://www.youtube.com/watch?v=1dats-1Efo> [27.9.2023]

¹² <https://support.spacewell.com/space/KB/14909472>, <https://support.spacewell.com/space/KB/14516256> [27.9.2023]

¹³ Figures © Spacewell. The figures serve as basis for the discussion of the corporate practices examined in this study. Sources: <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/space-monitor/>, <https://support.spacewell.com/space/KB/215154709/View+By+Space+%26gt%3B+%26quot%3BOccupancy%26quot%3B>, <https://support.spacewell.com/space/KB/492313/Prepare+your+sensor+plan> [26.9.2023]

2.1.1 Motion and presence detection

Figure 1 (center) shows a desk and room occupancy map for another office. To monitor employee presence in this particular office, the system uses 75 motion sensors, 16 “headcount” sensors and two “door count” sensors, according to Spacewell’s documentation.¹⁴ Figure 1 (right) shows the positions of the sensors installed in this particular office. The green circles and areas refer to motion sensors such as under-desk passive infrared (PIR) sensors,¹⁵ which detect heat emitted by human beings.¹⁶ The red circles refer to motion sensors that are installed in ceilings or in other places in the office, which count the number of people in a room or capture presence information about multiple distinct desks and workplaces. In addition, “door count” sensors can track how often a door was opened in the course of a day.¹⁷ The map in figure 1 (right) suggests that sensors are installed even at restroom doors.

2.1.2 Sensor hardware based on heat detection, visual analytics and other technologies

Spacewell does not sell its own sensor hardware. Employers can install different third-party sensors.¹⁸ This includes sensors from vendors the company refers to as “certified”,¹⁹ such as Browan,²⁰ Pointgrab, VergeSense, Airthings and Zens.²¹ The Browan motion sensor, for example, uses **passive infrared (PIR) technology**²² that detects heat and can be installed under desks.²³ VergeSense’s ceiling-mounted sensor can detect employee presence at up to eight distinct desks at once. It uses both PIR detection and a **visual sensor** that processes images of the room. VergeSense explains that it uses “low resolution” images (“352 x 288 pixel”) and “AI on device” to analyze room and desk occupancy.²⁴ While Spacewell emphasizes that the device does not allow for the extraction of the raw recorded images,²⁵ the system can still be considered a form of computer-vision-based video surveillance.

Spacewell recommends installing **additional sensors** that measure room temperature, humidity, barometric pressure, air quality, co2 levels and light intensity.²⁶ This data, which it refers to as “comfort data”, can be used to analyze room occupancy, as well. Spacewell explains, however, that the accuracy of occupancy tracking based on “comfort data” is low.²⁷ In addition, employers can use **parking sensors** based on magnetometers and radar technology to track parking lot occupancy,²⁸ as illustrated in figure 2 (right). Sensors can transmit the captured data to Spacewell’s cloud-based system either via Ethernet, Wi-fi²⁹ or “LoRa” technology, the latter of which uses wireless radio transmission similar to Wi-Fi but allows for longer ranges and lower power consumption.³⁰

¹⁴ <https://support.spacewell.com/space/KB/492313/Prepare+your+sensor+plan> [26.9.2023]

¹⁵ Supra note 11

¹⁶ See e.g. https://en.wikipedia.org/wiki/Passive_infrared_sensor

¹⁷ <https://support.spacewell.com/space/KB/492452> [28.9.2023]

¹⁸ <https://support.spacewell.com/space/KB/5242896> [27.9.2023]

¹⁹ <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/> [27.9.2023]

²⁰ <https://support.spacewell.com/space/KB/492410> [28.9.2023]

²¹ <https://support.spacewell.com/space/KB/492534/Install+%26amp%3B+Configure+Gateways+%26amp%3B+Sensors> [27.9.2023]

²² See e.g. https://en.wikipedia.org/wiki/Passive_infrared_sensor

²³ <https://support.spacewell.com/space/KB/491737> [28.7.2023]

²⁴ https://f.hubspotusercontent10.net/hubfs/8089267/VergeSense_DataSheet_L302.pdf [28.9.2023]

²⁵ <https://support.spacewell.com/space/KB/14516256> [27.9.2023]

²⁶ <https://support.spacewell.com/space/KB/15466506> [28.9.2023]

²⁷ Ibid.

²⁸ <https://support.spacewell.com/space/KB/50495489> [28.9.2023]

²⁹ <https://support.spacewell.com/space/KB/134119783> [28.9.2023]

³⁰ <https://support.spacewell.com/space/KB/14909465> [28.9.2023]

2.1.3 “Space monitoring” and “workplace analytics” for different purposes

Spacewell offers a range of analysis and reporting functionality based on desk and room occupancy data. Employers can use the “live data floorplan” and the “space monitor dashboard” to access real-time and historical occupancy data about buildings, floors, rooms and single desks (figure 2, left). According to Spacewell, “space monitoring” is an “essential part” of “workplace analytics”.³¹ Employers can use “granular space occupancy and utilization analysis” to “get a detailed picture of how the building is used during the day”, which includes “meeting rooms, desk seats, sanitary facilities, corridors, and even parking spaces”. Its technology “provides the objective insights needed to identify underused areas and improve space efficiency”. Employers can use it to “reduce underutilized space, save on rent, energy and cleaning, and optimize the workplace experience”.³² They can “watch changes that occur over a longer period at an accelerated rate”. They can “sit back and watch it as a movie” in order to “get a feeling of how presence, utilization, and comfort parameters evolve during the day” and “over multiple days”.³³

2.1.4 Room reservations, flexible desking and “smart” cleaning based on sensor data

Spacewell provides additional functionality for meeting room and desk booking.³⁴ Employers who do not assign desks and offices to employees but use flexible seating, sometimes called “hot desking” or “hoteling”,³⁵ can use the system to let employees book available desks and rooms themselves.³⁶ For this purpose, the system can display live maps that show occupied and available desks to employees via video display or smartphone app.³⁷ As figure 2 (center) indicates, it can show where particular named employees are currently located, down to individual desks and including small profile pictures. Employees can also search for colleagues on the map.³⁸

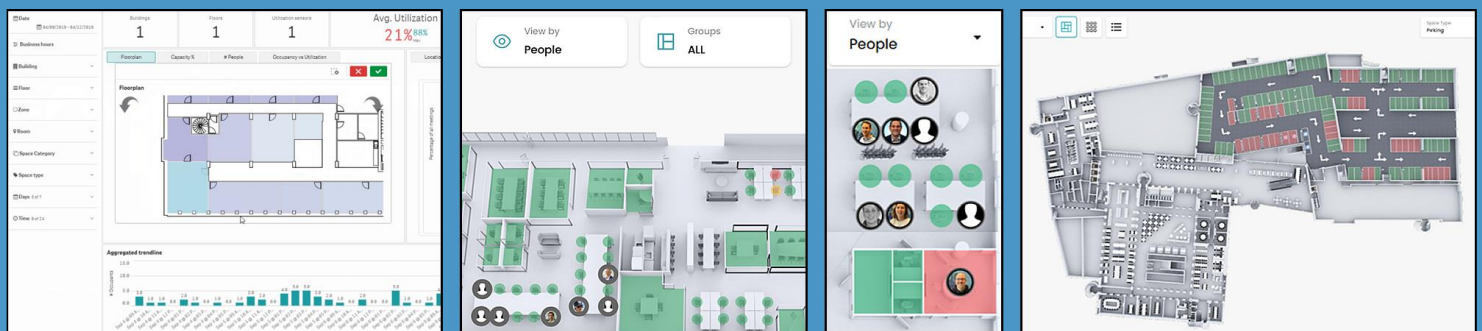


Figure 2: Monitoring desk, room and parking occupancy (Spacewell)³⁹

Spacewell emphasizes that the “utilization” data shown to employees generally comes from the room and desk

³¹ <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/> [28.9.2023]

³² Ibid.

³³ <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/space-monitor/> [26.9.2023]

³⁴ <https://spacewell.com/solutions/workplace-solutions/workplace-experience/> [28.9.2023]

³⁵ See e.g. https://en.wikipedia.org/wiki/Hot_desking, <https://en.wikipedia.org/wiki/Hoteling>

³⁶ <https://spacewell.com/resources/blog/hoteling-hot-desking-flexible-seating-and-hybrid-office/> [28.9.2023]

³⁷ <https://support.spacewell.com/space/KB/3768335> [28.9.2023]

³⁸ <https://support.spacewell.com/space/KB/147849646> [28.9.2023]

³⁹ Figures © Spacewell. The figures serve as basis for the discussion of the corporate practices examined in this study. Sources: <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/space-monitor/>, <https://support.spacewell.com/space/KB/226066433/View+By+Other+%26gt%3B+%26quot%3BPeople%26quot%3B>, <https://support.spacewell.com/space/KB/159973452/Live+Data+floorplan> [26.9.2023]

reservation system⁴⁰ and is not based on sensor-based “occupancy” data. Employers can, however, also make sensor-based occupancy data available to employees.⁴¹ They can customize whether employees are shown on the indoor map and in searches by default or not. Employees can override this default setting and “opt-out” of being shown or listed when they make room or desk reservations.⁴² In addition, Spacewell offers a “smart” task management application for office cleaning and other facility services that utilizes sensor-based occupancy data.⁴³

2.1.5 Privacy and data protection considerations

Although Spacewell is a European vendor, its extensive software documentation rarely addresses data protection with regard to employees.⁴⁴ Until recently, the company prominently explained that it uses “anonymous data capture”⁴⁵ and still uses this phrase on its website.⁴⁶ As the system processes extensive data from motion sensors that constantly monitor the presence of persons at desks over time, this is a questionable claim. When employees have assigned desks and offices, processing data about their presence at a desk can very likely be considered processing personal data under the GDPR, even more so when information about desk presence is displayed on indoor maps in real time and over time. When employers use Spacewell’s desk booking functionality, the system obviously processes personal data about who is seated at which desk. When the same system processes sensor-based data about desk presence, this can certainly also be considered processing personal data under the GDPR. At one point in the software documentation, Spacewell states that its system “doesn’t collect any personal information, especially where an open office policy is in place”. As detailed above, this is a questionable claim. Spacewell further states that the system “could indirectly collect personal information”, for example, “if each employee has his/her own workspace” and adds that “privacy concerns need to be evaluated” if the data “is combined with other data sources (such as a badging system) or is used by other services (such as Office 365)”.⁴⁷ While this acknowledges that employers can potentially directly or indirectly identify employees based on sensor-based presence data, these statements fall short of any meaningful engagement with the data protection risks posed by the system.

In January 2024, Spacewell added a function to “anonymize users”,⁴⁸ which promises to anonymize “personal data” on users after a configurable period of time. While this suggests that it acknowledges processing “personal data”, the notion of anonymization is questionable. The company explains that it removes usernames, names and email addresses for certain records, but still shows “reference” codes in the user interface, which suggests that it pseudonymizes data rather than anonymizing it.⁴⁹ Spacewell added another page in the documentation that addresses role-based access and a few other privacy and data protection topics.⁵⁰ The strongest protection from constant behavioral profiling based on monitoring desk presence is probably that the system appears to reduce the granularity of data collection to “15 minute time slots”.⁵¹ However, it stores “12 months of hourly sensor data”. Sensor data can “be exported for any selected time period” in order to be used in other reporting tools.⁵²

⁴⁰ <https://support.spacewell.com/space/KB/226066433/View+By+Other+%26gt%3B+%26quot%3BPeople%26quot%3B> [26.9.2023]

⁴¹ <https://support.spacewell.com/space/KB/77758583/Customizing+the+Workplace+App> [28.9.2023]

⁴² <https://support.spacewell.com/space/KB/160104537/GO+-+Profile+Settings> [28.9.2023]

⁴³ <https://spacewell.com/company/news/service-app-innovates-office-cleaning/> [28.9.2023]

⁴⁴ According to Google and the website’s search function: <https://support.spacewell.com/> [6.6.2024]

⁴⁵ <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/space-monitor/> [26.9.2023]

⁴⁶ <https://spacewell.com/solutions/workplace-solutions/workplace-experience/meetings-reservations/> [6.6.2024]

⁴⁷ <https://support.spacewell.com/space/KB/198049897/Hardware+Connectivity+%26amp%3B+Privacy> [28.9.2023]

⁴⁸ <https://support.spacewell.com/space/WN/410353665/24+-+January+release> [6.6.2024]

⁴⁹ <https://support.spacewell.com/space/KB/451936369/Anonymizing+data> [6.6.2024]

⁵⁰ <https://support.spacewell.com/space/KB/485883931/How+Spacewell%60s+Development+Practices++Your+Data> [6.6.2024]

⁵¹ <https://support.spacewell.com/space/KB/492245/Sensor+troubleshooting+guide> [28.9.2023]

⁵² <https://spacewell.com/solutions/workplace-solutions/workplace-analytics/space-monitor/> [26.9.2023]

2.2 Locatee – behavioral profiling based on motion sensor, badge and device location data

The Swiss vendor Locatee also offers workplace analytics software that utilizes occupancy data.⁵³ In addition to sensors that monitor “employee presence”, it uses **badge data** and **device data** collected via the employer’s network infrastructure.⁵⁴ While sensors mounted in various places in the office “provide the most precise and granular level of data”, the “advantage” of using badge data “is that it relies on technologies which are often already in place”, according to Locatee.⁵⁵ As Wi-Fi and LAN data can provide “continuous and real-time data on the whereabouts of a device”, a company’s existing Wi-Fi and LAN network infrastructure can be used to measure “occupancy through device location”.⁵⁶ Indoor location tracking via device data is further addressed in section 3.

2.2.1 Analyzing employee and team behaviors

Figure 3 (top left) shows a “heat map” of an office, as displayed by Locatee’s analytics software. It indicates “how often each workstation was used in a given period”, with the term workstation referring to desks or seats at desks.⁵⁷

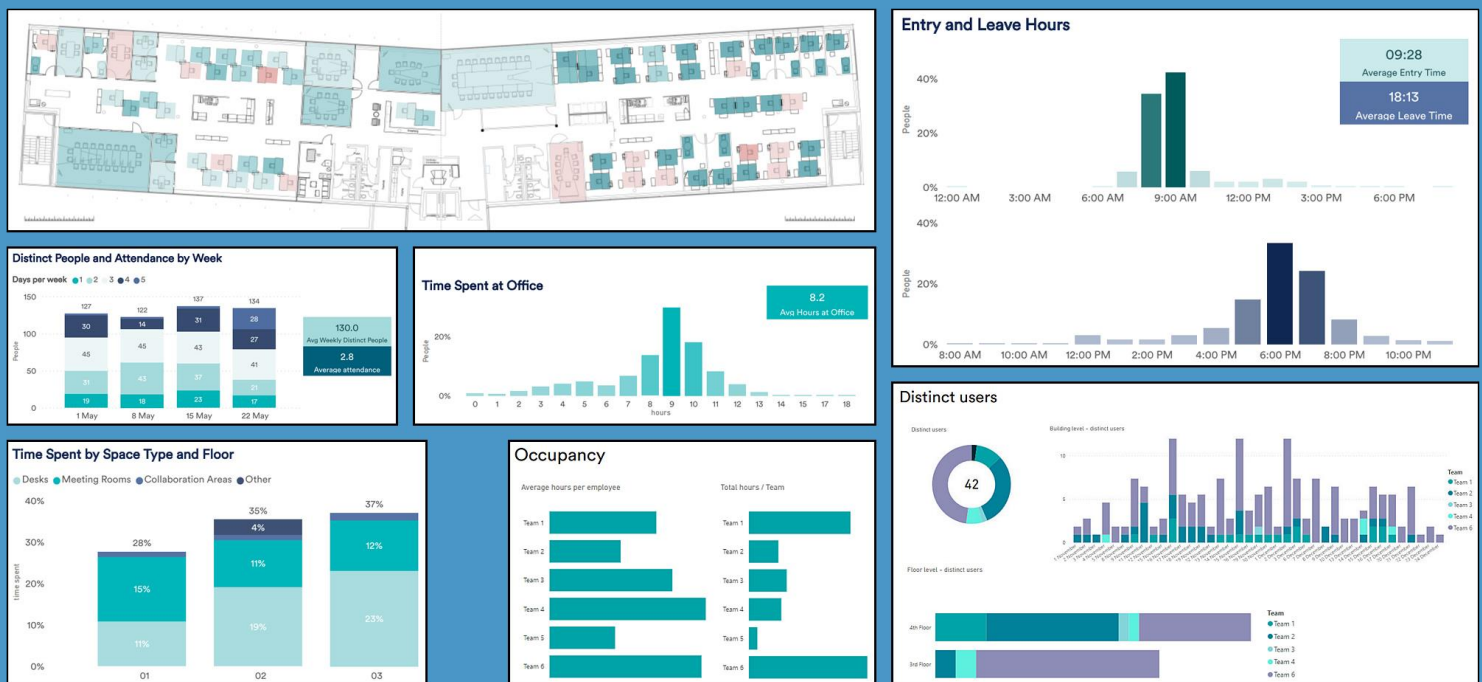


Figure 3: Monitoring desk occupancy for teams, entry and leave hours, time spent at office (Locatee)⁵⁸

⁵³ <https://locatee.com/en/> [29.9.2023]

⁵⁴ <https://locatee.com/en/sources-we-integrate/>, <https://cdn2.hubspot.net/hubfs/1297155/Measurement-Methods-of-Space-Utilisation-1.pdf> [29.9.2023]

⁵⁵ Ibid.

⁵⁶ Ibid.

⁵⁷ <https://locatee.com/en/blog-post/returning-to-workplace-post-pandemic/> [27.9.2023]

⁵⁸ Figures © Locatee. The figures serve as basis for the discussion of the corporate practices examined in this study. Sources: <https://locatee.com/en/blog-post/returning-to-workplace-post-pandemic/>, <https://locatee.com/wp-content/uploads/2023/04/Sample-Spotlight-Report-2.pdf>, <https://locatee.com/wp-content/uploads/2022/11/Team-Analytics-Report-A.pdf> [27.9.2023]

Furthermore, figure 3 shows various **reports** provided by the vendor. Locatee states that its reports include “utilization insights”, “people behavior metrics” and information about “people presence enriched with team information”.⁵⁹ Employers can analyze, for example, how many employees went to the office each day and how many days a week they come to the office, on average (“Distinct People and Attendance by Week”). They can analyze how many hours employees spend in the office per day, on average (“Time Spent At Office”), at which time they enter and leave the office, on average (“Entry and Leave Hours”) and how much time they spend per floor and on their desks, in meeting rooms and other space types (“Time Spent by Space Type and Floor”).⁶⁰

As illustrated in figure 3 (bottom center and right), Locatee also provides “**team analytics**” reports.⁶¹ Employers can, for example, analyze how many hours employees who are members of different teams spend in the office, both on average and in total (“Occupancy”). The example report suggests that employees in “Team 5” spend the least time in the office. Another report shows how much time members in different teams spend on each floor in the office (“Distinct users”). In a promotional video, a Locatee representative demonstrates how employers can use the team analytics functionality.⁶² The presenter is wondering whether members of a particular team, the “innovation department”, are really using their assigned spaces. The example report in the video shows that 11 employees spent 176 hours on an office’s first floor, six of them from the innovation department. Five members from the innovation department spent 32 hours in another office building. The presenter concludes that “they’re not even in this building. They’re somewhere else”.⁶³ These examples show that while Locatee’s reports analyze occupancy data at the aggregate level, they reveal extensive information about employee behavior, including about small groups. Employers can potentially use the reports to further investigate behaviors they consider to be undesirable.

2.3 Practical examples and worker resistance

On a Monday in January 2016, the staff of the UK newspaper **The Daily Telegraph** discovered small boxes under their desks, which turned out to be motion sensors. According to a media report, management told staff that the sensors, installed over the weekend without notice, would remain under the desks for four weeks to analyze desk usage in order to improve “energy efficiency”. After sustained criticism, the sensors were removed the same day.⁶⁴ Something similar happened at the UK bank **Barclays**.⁶⁵ In both cases, employers used motion sensors from the vendor **OccuEye**, which was acquired by the facility and workplace vendor **FM:Systems** in 2019.⁶⁶ The company provides sensor-based workplace analytics technology that promises to track “employee attendance” and “real-time occupancy”.⁶⁷ FM:Systems states that it has “deployed” 250,000 sensors at the sites of 1,200 clients across 80 countries.⁶⁸ As of 2022, the company’s website suggested that FM:Systems itself had access to office occupancy data from employers in the US, UK, Ireland, France, Italy, Belgium, Norway, Hungary and other countries and used the data to publish aggregate analysis results for its own promotional purposes.⁶⁹

⁵⁹ <https://locatee.com/en/locatee-reports/> [29.9.2023]

⁶⁰ <https://locatee.com/wp-content/uploads/2023/04/Sample-Spotlight-Report-2.pdf> [27.9.2023]

⁶¹ <https://locatee.com/wp-content/uploads/2022/11/Team-Analytics-Report-A.pdf> [27.9.2023]

⁶² Next Level Hybrid Work with Locatee, 31.3.2022. Video from min 26:10: <https://locatee.com/en/resource/next-level-hybrid-work-with-locatee/>, <https://vimeo.com/694385090> [29.9.2023]

⁶³ Ibid.

⁶⁴ <https://www.theguardian.com/media/2016/jan/11/daily-telegraph-to-withdraw-devices-monitoring-time-at-desk-after-criticism>

⁶⁵ <https://www.bloomberg.com/news/articles/2017-08-18/barclays-puts-in-sensors-to-see-which-bankers-are-at-their-desks>

⁶⁶ <https://fmsystems.com/news/verdantix-fmsystems-is-rebranding-its-product-offerings-as-a-digital-workplace-solutions-suite/> [29.9.2023]

⁶⁷ <https://fmsystems.com/products/workplace-analytics/> [29.9.2023]

⁶⁸ <https://fmsystems.com/> [29.9.2023]

⁶⁹ <https://web.archive.org/web/20220419204352/https://fmsystems.com/our-resources/covid-19-coronavirus/space-data-visualization/>

In 2022, the US-based **Northeastern University** installed motion sensors under the desks of graduate student workers.⁷⁰ Once again, this occurred overnight and without their consent.⁷¹ The incident led to protests on the campus and was widely reported via social media.⁷² While the university claimed that it wanted to conduct a study on desk usage, one affected worker responded that they have assigned desks and use key cards to get into their rooms, which would already provide enough data for this purpose. Student workers considered the motion sensors to be “intimidating” and “unnecessary” surveillance that serve “no scientific purpose”.⁷³ They removed the sensors from their desks and used them to form the letters “NO”, as shown in figure 4 (top right). The university stopped the project.⁷⁴

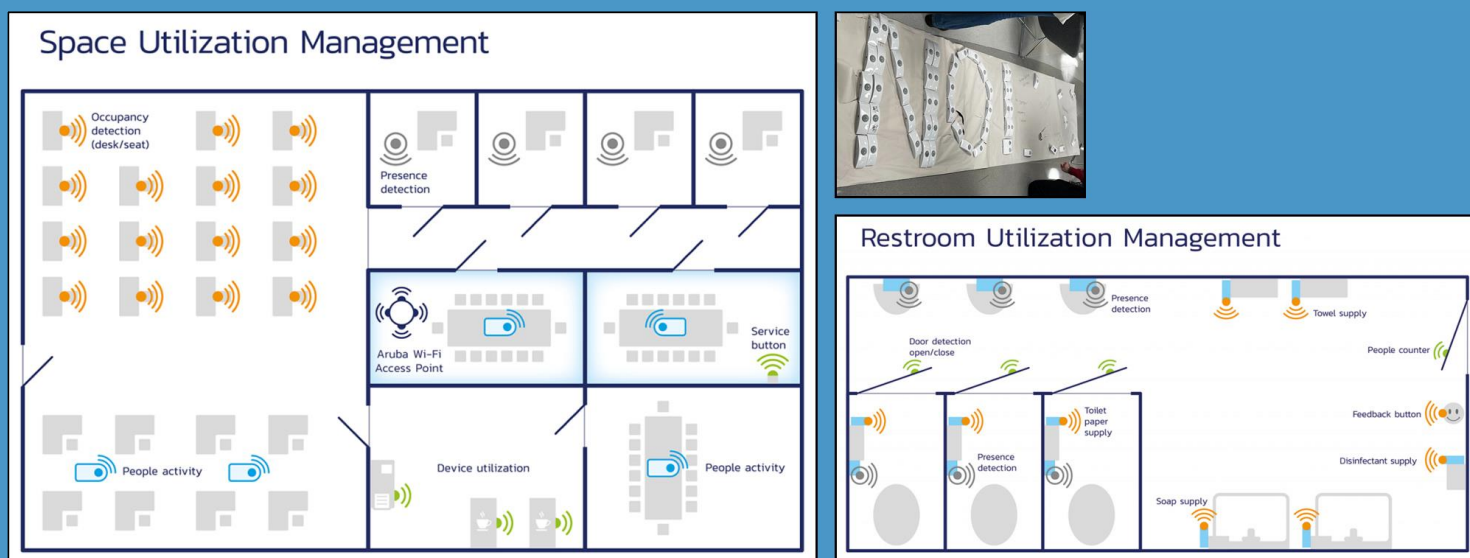


Figure 4: Monitoring office and restroom utilization (EnOcean/Aruba), protest against desk monitoring⁷⁵

The under-desk motion sensors installed at the university came from **EnOcean**,⁷⁶ a German “smart” device vendor.⁷⁷ Figure 4 (left) illustrates how EnOcean promotes “space utilization” technology for offices, which relies on EnOcean sensors and Aruba Wi-Fi routers. The floorplan shows occupancy sensors installed at desks and “people activity” and “presence detection” sensors installed in meeting rooms and other areas in an office. Figure 4 (right) shows “presence detection”, “people counter” and “door detection” sensors installed in a restroom.⁷⁸

⁷⁰ <https://www.vice.com/en/article/m7gwy3/no-grad-students-analyze-hack-and-remove-under-desk-surveillance-devices-designed-to-track-them>

⁷¹ <https://news.techworkerscoalition.org/2022/11/29/issue-19/> [29.9.2023]

⁷² e.g. <https://twitter.com/maxvonhippel/status/1578048652215431168>, https://www.reddit.com/r/NEU/comments/xx7d7p/northeastern_graduate_students_privacy_is_being/ [29.9.2023]

⁷³ <https://news.techworkerscoalition.org/2022/11/29/issue-19/> [29.9.2023]

⁷⁴ <https://www.vice.com/en/article/m7gwy3/no-grad-students-analyze-hack-and-remove-under-desk-surveillance-devices-designed-to-track-them>

⁷⁵ Figures © EnOcean/Aruba, Tech Workers Coalition. The figures serve as basis for the discussion of the corporate practices examined in this study. Sources: <https://www.enocean.com/en/applications/partnerships/aruba/>, <https://news.techworkerscoalition.org/2022/11/29/issue-19/> [26.9.2023]

⁷⁶ <https://news.techworkerscoalition.org/2022/11/29/issue-19/> [29.9.2023]

⁷⁷ <https://www.enocean.com/en/about-us/about-enocean/> [29.9.2023]

⁷⁸ <https://www.enocean.com/en/applications/partnerships/aruba/> [26.9.2023]

3. Tracking indoor location, movements and behaviors

This section examines technologies and software systems that allow organizations to locate employees, customers and other persons inside buildings, analyze their movements and profile their behaviors.

3.1 Indoor location tracking

As GPS technology is too imprecise and unreliable indoors, a number of other technologies have emerged that make it possible to track the location of objects or people inside buildings. Most prominently, Wi-Fi networks that provide internet connectivity for laptops, smartphones, tablets and other networked devices can also be used to track the location of devices that are connected to Wi-Fi access points. Similarly, other wireless networking technologies based on radio transmission can be turned into location tracking systems – for example, Bluetooth and more specifically “Bluetooth Low Energy” (BLE). Location tracking based on BLE technology can require a fairly complex setup where BLE-enabled mobile devices (e.g. smartphones, wearables, employee badges, “beacons” and “tags” attached to mobile objects like tools, vehicles or goods) interact with BLE-enabled devices that are permanently installed at certain places in a building. While the accuracy of indoor location tracking based on Wi-Fi and BLE is reported to be around 1-5 meters, another wireless technology which is referred to as “ultra-wideband” (UWB) is considered to provide an accuracy of 0.5 meters. In addition, radio-frequency identification (RFID) technology, which has been used to locate objects for decades, still plays a role (Curran et al., 2011; Kriz et al., 2016; Thiede et al., 2021).

Several vendors offer **real-time locating systems (RTLS)**, which utilize one or several of these technologies to track the location of people and objects inside buildings such as offices, factories, warehouses or retail stores. According to the market research firm Gartner, this includes major networking technology firms such as Cisco and Juniper Networks. Other relevant vendors in indoor location tracking include Zebra Technologies, Inpixon, Ubisense, Kontakt.io and the security services firm Securitas.⁷⁹ Employers use these systems to track the movements and behaviors of workers for different purposes.

3.2 Turning Cisco’s network infrastructure into a location tracking system

The network technology giant Cisco offers a product that turns Wi-Fi access points and other wireless networking infrastructure installed in a building into a system that tracks the location of employees, customers, devices and other objects for a wide range of purposes. Cisco refers to its cloud-based location tracking platform as “Cisco Spaces”.⁸⁰ The platform allows companies to “gain insights into how people and things move throughout their physical spaces”⁸¹ and “understand the behavior and location of people (visitors, employees) and things (assets, sensors)”⁸². Companies can get a “real time view of the behavior of employees, guests, customers and visitors”⁸³ and “profile” them “based on at-location behavior”⁸⁴ in order to “get a detailed picture of their behavior”.⁸⁵ In total,

⁷⁹ Gartner (2023): Magic Quadrant for Indoor Location Services. Gartner, 21.2.2023

⁸⁰ “Cisco Spaces”, formerly “Cisco DNA Spaces”: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-spaces/index.html> [30.9.2023]

⁸¹ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/q-and-a-c67-741795.html> [30.9.2023]

⁸² <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

⁸³ <https://spaces.cisco.com/home/> [30.9.2023]

⁸⁴ <https://www.cisco.com/c/en/us/products/collateral/wireless/dna-spaces/datasheet-c78-741786.html> [30.9.2023]

⁸⁵ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

Cisco's location tracking platform has so far processed 17.2 trillion "location data points" collected via 3.1 million Wi-Fi access points installed at more than 250,000 buildings, according to the company.⁸⁶

3.2.1 Indoor location tracking via Wi-Fi and BLE technology

Cisco Spaces can track the location of laptops, smartphones and other networked devices via Cisco's Wi-Fi access points.⁸⁷ Additionally, it can use BLE technology to track the location of BLE-enabled devices.⁸⁸ Figure 5 (left) illustrates how the system displays the location of devices in an office on an indoor map. The map in this example shows the location of 11 "clients", which represent the tracked devices and are displayed as small green icons shaped like a simplified person. According to the map, two persons are currently located at particular coordinates in room "3108". Another person is, for example, located at a particular place in the corridor next to the room. The larger blue icons represent the wireless access points, which track the location of "client" devices connected to them, and thus the persons who carry these devices.

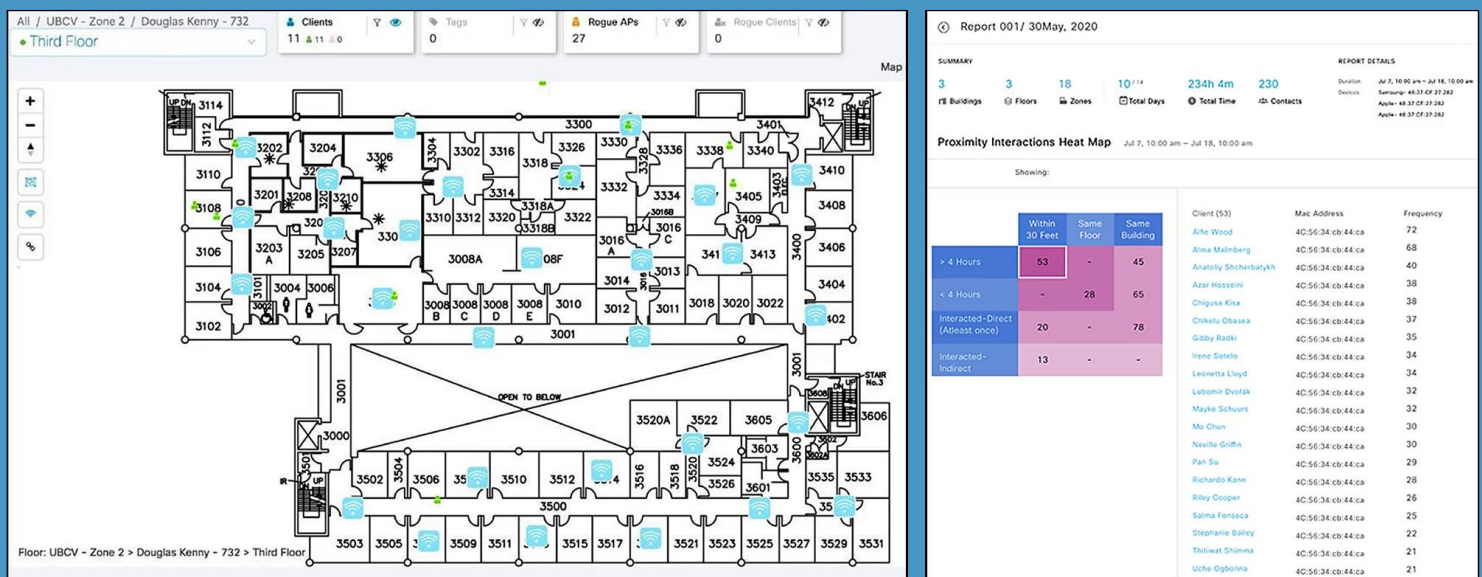


Figure 5: Indoor location tracking map and analysis of device proximity across named employees (Cisco)⁸⁹

As figure 6 (left) illustrates, employers can use Cisco Spaces to **process location data at a massive scale** and frequency. The example report suggests that the system processed millions of "location updates" about 138 persons who visited a building, which was collected via 11 wireless access points.⁹⁰ Figure 6 (center) shows a report that displays the current number of visitors in a building in real time,⁹¹ broken down by the type of located devices

⁸⁶ <https://spaces.cisco.com/> [30.9.2023]

⁸⁷ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html>, <https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m-product-overview.html> [29.9.2023]

⁸⁸ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html>, <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/q-and-a-c67-741795.html>, https://documentation.meraki.com/MR/Monitoring_and_Reporting/Location_Deployment_Guidelines [29.9.2023]

⁸⁹ Figures © Cisco. The figures serve as basis for the discussion of the corporate practices examined in this study. Source:

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

⁹⁰ <https://www.cisco.com/c/en/us/td/docs/wireless/spaces/config-guide/ciscospaces-configuration-guide/m-home.html> [2.10.2023]

⁹¹ https://www.cisco.com/c/en/us/td/docs/wireless/spaces/config-guide/ciscospaces-configuration-guide/m_rightnow.html [2.10.2023]

(“WiFi devices”, “BLE devices”) and the category of located persons (“employee”, “student”, “guest”). This example report, which appears to refer to a university building, states that it detects the type of visitor by “SSID category”, which suggests that the system recognizes employees, students and guests because they connect to different Wi-Fi networks.⁹²

3.2.2 Behavioral profiling based on location data

The “location personas” module in Cisco Spaces provides additional functionality for behavioral profiling. Companies can identify groups of visitors in a building “based on their at-location behavioral attributes” in order to “target” them in certain ways.⁹³ As figure 6 (right top) illustrates, a company can, for example, identify certain groups of customers who visit their building (“weekend lunch visitors”, “weekday lunch visitors”). It can also identify employees in order to deliberately target or exclude them (“detect employee devices”, “filter employee devices”).

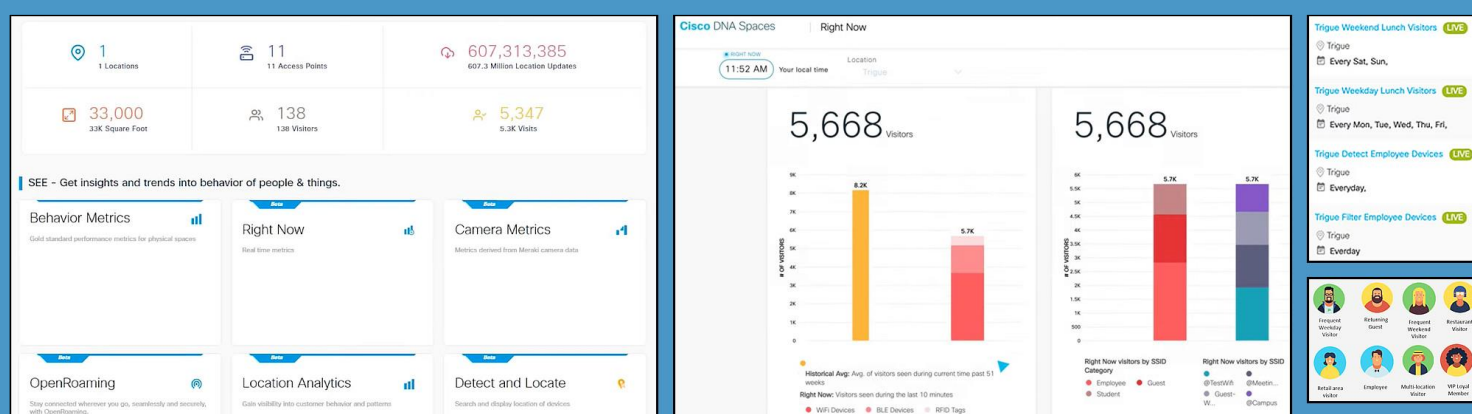


Figure 6: Indoor location tracking reports and behavioral profiling (Cisco)⁹⁴

Figure 6 (right bottom) shows other “location personas” as suggested by Cisco (e.g. “restaurant visitor”, “retail area visitor”, “VIP loyal member”, “returning guest”, “employee”). Section 3.2.5 further describes how companies can use these profiles to target customers or employees with promotions or notifications that aim to change their behavior.

3.2.3 Analyzing movements and behaviors at the individual level

While the reports described in section 3.2.1 show aggregate metrics about visitors in a building, Cisco Spaces is well equipped to analyze indoor movements and behaviors of named employees at the individual level. During the coronavirus pandemic, Cisco introduced a “proximity reporting” system that allows employers to “understand

⁹² The “SSID” or “network name” is a “unique identifier that wireless clients can connect to or share among all devices in a wireless network”: <https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5169-wireless-access-points-glossary-of-terms.html> [2.10.2023]

⁹³ <https://spaces.cisco.com/store/product/location-personas/> [2.10.2023]

⁹⁴ Figures © Cisco. The figures serve as basis for the discussion of the corporate practices examined in this study. Sources: Cisco YouTube channel, "Cisco DNA Spaces Episode 1. Overview", 21.5.2021, min 0:40: <https://www.youtube.com/watch?v=SxZgrCr2IA>; Cisco YouTube channel, "Cisco Spaces for Trusted Workplace Demo", 27.7.2021, min 1:19: <https://www.youtube.com/watch?v=NikuY3bfWRQ>, <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html>, <https://spaces.cisco.com/store/product/location-personas/> [29.9.2023]

where an individual has been if they reported exposure to or infection by the virus”. They can also see which employees were in the same spaces at the same time.⁹⁵ Figure 5 (right) shows a report about an employee’s past interactions with other employees. The employee in this example spent 234 hours in three buildings and three floors over the previous ten days. They spent more than four hours within “30 feet” of 53 other employees and directly interacted with 20 employees. The report also shows a list of named employees including a unique device identifier (“MAC address”⁹⁶) and the number of their interactions with the employee affected by the virus. This application, which is far more intrusive than the privacy-preserving contact tracing system implemented by Google and Apple during the pandemic,⁹⁷ shows that Cisco Spaces can be used for far-reaching behavioral monitoring.

Cisco Spaces generally allows employers to access detailed information about the location of devices. As figure 7 (left) illustrates, the “detect and locate” functionality⁹⁸ can display the **current and past locations** of each “client” device detected in a building. The indoor map in this example shows a large number of detected devices, which are represented by the green dots. Clicking on a device reveals additional details about it, including its exact indoor coordinates, a coarse description of its location and device identifiers like its MAC and IP address.⁹⁹

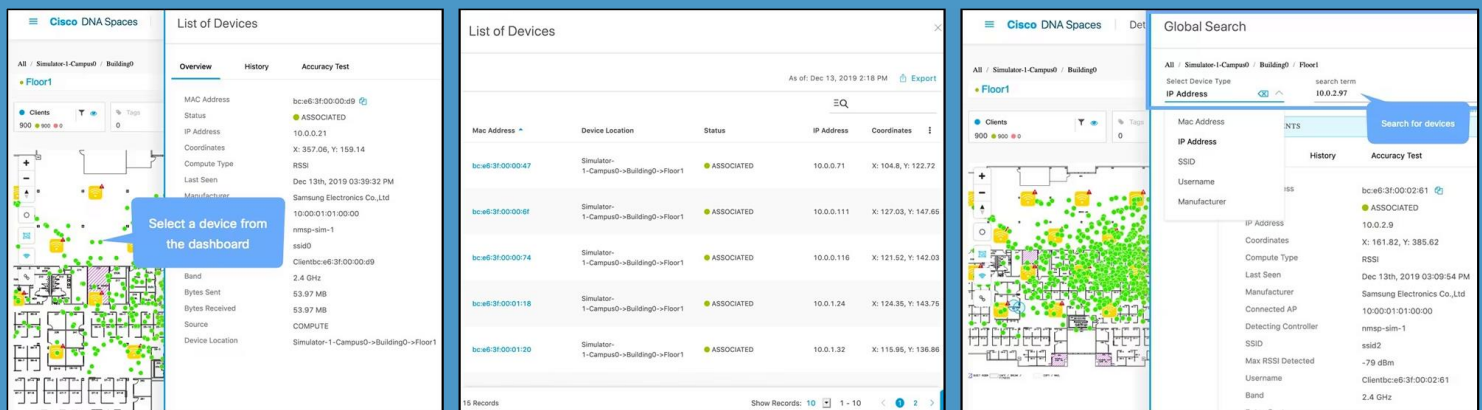


Figure 7: Accessing current and past locations of devices, searching for devices (Cisco)¹⁰⁰

The list of detected devices provides similar information (figure 7, center). The “client history” reveals past locations and movements of a device.¹⁰¹ The systems allows **searching for devices** by device identifier and “username” (figure 7, right).¹⁰² Section 3.2.6 further describes how the system can identify the employees who use these devices.

3.2.4 Tracking indoor behavior with Cisco’s security cameras and WebEx devices

In addition to Wi-Fi access points and BLE technology, Cisco Spaces can also use data derived from its Meraki video cameras to analyze the “behavior of people within physical spaces”, for example, by tracking the number of

⁹⁵ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

⁹⁶ See e.g. https://en.wikipedia.org/wiki/MAC_address

⁹⁷ See e.g. <https://covid19.apple.com/contacttracing>

⁹⁸ <https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m-product-overview.html> [2.10.2023]

⁹⁹ https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m_clienthistory.html [2.10.2023]

¹⁰⁰ Figures © Cisco. The figures serve as basis for the discussion of the corporate practices examined in this study. Sources:

https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m_clienthistory.html,

https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m_map.htm, <https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/locationaccuracy.html> [29.9.2023]

¹⁰¹ Ibid.

¹⁰² https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m_globalsearch.html [2.10.2023]

persons staying in a space, entering or exiting it.¹⁰³ Cisco refers to its Meraki video cameras as “cloud-based security cameras”.¹⁰⁴ They provide video analytics and computer vision functionality that promises to automate “people and vehicle detection”.¹⁰⁵ As such, Cisco Spaces repurposes data from a highly intrusive video surveillance system originally recorded for security and safety purposes for the analysis of indoor movements. The system can also integrate Cisco’s WebEx video conferencing and collaboration devices. Cisco tells its clients that the Spaces platform “turns your Cisco hardware (Catalyst, Meraki, WebEx) into sensors”. It “captures location signals from people and things within your buildings” by “leveraging your Cisco Network Infrastructure – Access Points, Switches, Cameras, Collab devices & Third Party IoT sensors”.¹⁰⁶

3.2.5 Applications for Cisco’s location tracking system

Cisco promotes a wide range of applications for its indoor location platform that affect customers and employees:

- **Location data on customers.** Retailers, restaurants, hotels, event venues, airports, universities and hospitals can use Cisco Spaces to analyze the movements and behaviors of both employees and other persons (e.g. customers, shoppers, guests, visitors, students, patients) inside their buildings.¹⁰⁷ They can do so to make decisions about these spaces and the services they offer.¹⁰⁸ They can profile and target customers with promotions, personalized messages or recommendations via mobile apps based on their movement patterns and measure the impact of campaigns.¹⁰⁹ Companies can directly identify visitors by requiring them to enter email addresses and other identifying information when connecting to a building’s Wi-Fi network.¹¹⁰ Hospitals and airports can provide additional services to visitors such as indoor navigation.¹¹¹ Universities can use the system to track student attendance and “automate participation grading”.¹¹² According to Cisco, employers can also use customer location data to make decisions about employees, for example, to make “informed and efficient changes to staff and cleaning schedules”.¹¹³
- **Location data on employees.** Employers can use Cisco Spaces to turn offices into “smart workplaces”.¹¹⁴ This includes occupancy monitoring, meeting room management and other similar applications as described in section 2. In contrast to occupancy monitoring and presence detection based on motion sensors, tracking the movements of employees based on their devices provides even more extensive insights about their behaviors. Employers can access reports that display aggregate data about employees’ entry and exit times, workday durations, visit durations by floor and other “behavior metrics”.¹¹⁵ They can profile employees,¹¹⁶ send them

¹⁰³ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

¹⁰⁴ <https://meraki.cisco.com/products/smart-cameras/> [2.10.2023]

¹⁰⁵ <https://meraki.cisco.com/products/smart-cameras/video-analytics/> [2.10.2023]

¹⁰⁶ <https://spaces.cisco.com/> [30.9.2023]

¹⁰⁷ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html>, <https://spaces.cisco.com/stadium-venue-solutions/>, <https://spaces.cisco.com/airport/> [2.10.2023]

¹⁰⁸ Ibid.

¹⁰⁹ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html>, <https://spaces.cisco.com/digital-experience/> [2.10.2023]

¹¹⁰ <https://spaces.cisco.com/store/product/captive-portals/> [2.10.2023]

¹¹¹ <https://spaces.cisco.com/indoor-navigation/> [2.10.2023]

¹¹² <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

¹¹³ <https://spaces.cisco.com/retail/> [2.10.2023]

¹¹⁴ <https://spaces.cisco.com/smart-workspaces/> [2.10.2023]

¹¹⁵ https://www.cisco.com/c/en/us/td/docs/wireless/spaces/config-guide/ciscospaces-configuration-guide/m_business-insights.html [2.10.2023]

¹¹⁶ <https://spaces.cisco.com/store/product/location-personas/> [2.10.2023]

“contextual notifications” based on their movements and measure the impact of campaigns that aim to change their behavior.¹¹⁷

- Employers in manufacturing can use Cisco Spaces to “understand employee behavior that affects performance”¹¹⁸ and to analyze “dwell times, frequency of visits, patterns of employees”. They can use the system to improve security and safety, for example by “receiving alerts when equipment like forklifts leave the facility or enter restricted zones”.¹¹⁹ Hospitals can use it for “patient tracking”, “fall detection, infant tracking and real-time environmental monitoring”,¹²⁰ but also to provide a “panic button for staff safety” and “automate monitoring and reporting of hand hygiene compliance”.¹²¹ Retailers can detect “any deviance from usual asset usage and location”.¹²² Employers can use the system for “loss prevention” purposes in cybersecurity.¹²³ Generally, Cisco promotes the use of its location tracking system for occupational health purposes, from measuring room occupation density to proximity tracing.¹²⁴

3.2.6 Privacy and data protection considerations

The previous sections show that employers can use the Cisco Spaces platform to collect, analyze and utilize **extensive personal data about the movements and behaviors of employees** and other persons inside buildings. Aggregate reports may still rely on extensive personal data processing.

Cisco provides a “privacy data sheet” for its cloud-based Spaces platform, which explains how Cisco itself processes personal data as a “data processor” on behalf of its corporate customers.¹²⁵ According to the document, the platform processes data about “end user behavior”, such as location and visit duration, in combination with MAC addresses, which represent pseudonymous identifiers referring to tracked devices and their users. MAC addresses are collected “by default”. It also collects IP addresses and it may collect “employee username” and “userid” information about persons who are connected to Cisco’s network infrastructure, the latter of which can be “pseudonymized” or “hashed” in “some instances”. Optionally, the MAC address can also be “hashed” and there is an option to “skip sending IP addresses” to Cisco Spaces. In a section about “certifications and compliance with privacy requirements”, Cisco claims that the platform provides “GDPR compliance”, whatever that means.¹²⁶

According to promotional materials, the platform supports “MAC randomization”, which “limits user tracking and supports privacy requirements”. Cisco emphasizes, however, that this option will render location analytics “unreliable” and make certain applications impossible.¹²⁷ As soon as employers use functionality to **track, profile, target or otherwise single out individual devices or even named persons** over time, this requires processing a stable pseudonymous identifier referring to devices or persons. Cisco Spaces provides the option to exclude certain areas

¹¹⁷ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

¹¹⁸ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

¹¹⁹ <https://spaces.cisco.com/manufacturing/> [2.10.2023]

¹²⁰ <https://spaces.cisco.com/smart-healthcare/> [2.10.2023]

¹²¹ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

¹²² <https://spaces.cisco.com/retail/> [2.10.2023]

¹²³ <https://spaces.cisco.com/detect-locate/> [2.10.2023]

¹²⁴ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

¹²⁵ <https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/DNA/cisco-dna-spaces-privacy-data-sheet.pdf> [2.10.2023]

¹²⁶ Ibid.

¹²⁷ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

in a building from location tracking.¹²⁸ The company emphasizes that employers can export location data to “correlate” it “with other data sources”¹²⁹ and “integrate” the platform with other “enterprise systems”, such as “building management systems” and “human resource management systems”, to “drive outcomes from external systems”.¹³⁰

Cisco offers employers the ability to compare behavioral metrics with average values for the industry to which the business belongs, based on “data obtained from other clients who have installed Cisco Spaces”.¹³¹ This suggests that Cisco **processes personal data across clients** for the purpose of calculating industry benchmarks. According to its “privacy data sheet”, Cisco Spaces collects “system information” to “assist Cisco with understanding product usage and enabling product improvements”. It also collects “telemetry data” such as “Device Mac Address”, “Network data”, “Network SSID”, “Client Device Location Details (X, Y)” and “Network Hierarchy” including information about buildings and floors.¹³² The GDPR legal basis and purposes of processing this data for Cisco’s own purposes or to calculate industry benchmarks are not entirely clear.

3.2.7 Third-party applications based on Cisco Spaces

Like other cloud-based platforms, Cisco Spaces offers an “app store” which provides applications from third-party vendors that offer additional functionality or which integrate the platform with other systems.¹³³ For example, the Swiss workplace analytics and occupancy monitoring vendor **Locatee**, which is examined in section 2.2, provides an application that enables it to analyze indoor location data collected via the Cisco Spaces platform.¹³⁴ **IBM** also offers an application named “Tririga Building Insights” that utilizes Cisco Spaces data and “AI” to analyze how employees use offices, rooms and desks and how they move in buildings.¹³⁵ IBM’s system provides an “anomaly detection model” that promises to detect office occupancy patterns that deviate from “normal” patterns in order to exclude “peaks and lows due to special events” from utilization metrics.¹³⁶

3.3 Locating nurses, security guards and sales associates with Juniper Networks

Juniper Networks, another network technology giant, offers a cloud-based location tracking platform similar to Cisco’s system.¹³⁷ With Juniper’s platform, which uses Wi-Fi and BLE technology to “deliver location services accurate to between one and three meters”,¹³⁸ employers can analyze “data going back up to 13 months or more to identify trends and perform long-term historical time series analyses of network, app, employee, and guest behavior”.¹³⁹ The company’s “Mist Asset Visibility” product uses BLE technology integrated in Juniper’s Wi-Fi access points to “find key assets and people using detailed location analytics”.¹⁴⁰ Employers can use it to “locate key human resources such as nurses, security guards, and sales associates” via their mobile devices or BLE-enabled badges.¹⁴¹

¹²⁸ https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m_map.html [2.10.2023]

¹²⁹ <https://spaces.cisco.com/home/> [30.9.2023]

¹³⁰ <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/solution-overview-c22-742158.html> [29.9.2023]

¹³¹ https://www.cisco.com/c/en/us/td/docs/wireless/spaces/config-guide/ciscospaces-configuration-guide/m_business-insights.html [2.10.2023]

¹³² <https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/DNA/cisco-dna-spaces-privacy-data-sheet.pdf> [2.10.2023]

¹³³ <https://spaces.cisco.com/store/> [2.10.2023]

¹³⁴ <https://spaces.cisco.com/store/product/locatee-ch/> [2.10.2023]

¹³⁵ <https://spaces.cisco.com/store/product/ibm-tririga-building-insights/> [2.10.2023]

¹³⁶ <https://www.ibm.com/docs/en/tbi?topic=overview-ai-analytical-models> [2.10.2023]

¹³⁷ <https://www.juniper.net/us/en/solutions/indoor-location.html> [2.10.2023]

¹³⁸ Ibid.

¹³⁹ <https://www.juniper.net/us/en/products/cloud-services/premium-analytics.html> [2.10.2023]

¹⁴⁰ <https://www.juniper.net/us/en/products/cloud-services/asset-visibility.html> [2.10.2023]

¹⁴¹ Ibid.

Figure 8 (left) illustrates how the system can display the location of “client” devices on a real-time indoor map. The tracked devices can be assigned “names” based on their MAC address and other device identifiers.¹⁴²

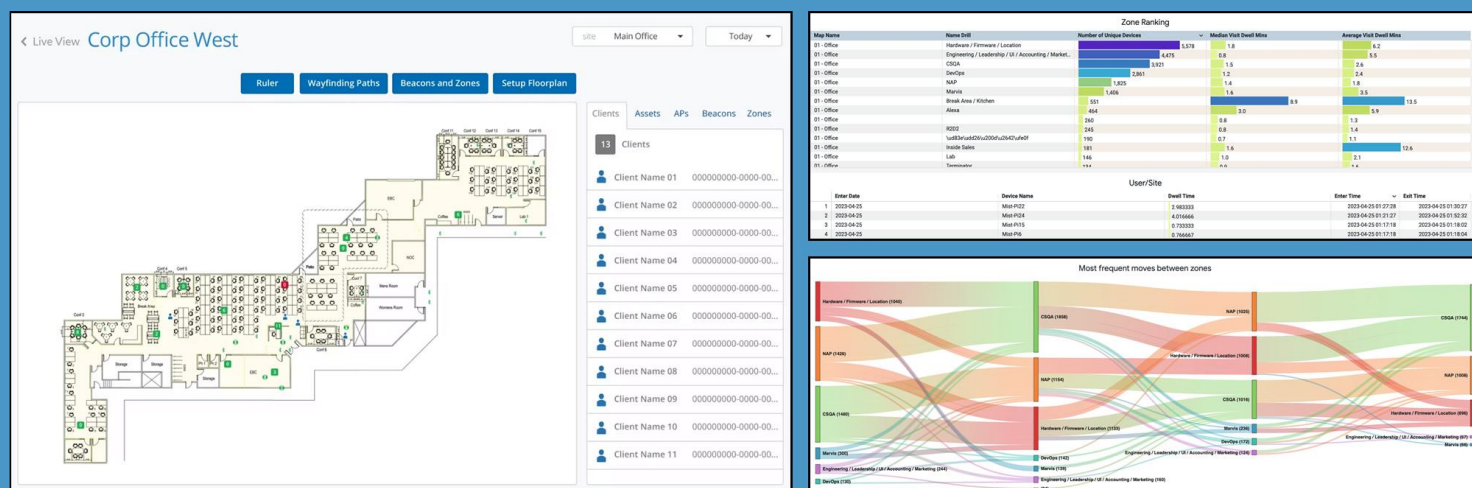


Figure 8: Indoor location tracking map and reports about employee behavior (Juniper)¹⁴³

Juniper’s system provides several reports that offer insights into how employees move inside offices and other buildings, based on Wi-Fi and BLE data. Figure 8 (top right) shows a report that displays information about the number of “unique devices” that visited certain “zones” in a building, including the median and average duration of those visits. In this example, 551 employee devices visited the “break area / kitchen” zone, with an average duration of 13.5 minutes per visit. The same report also displays a list of each visit at the individual level, including the “device name” and the exact “enter” and “exit” times. As shown in figure 8 (bottom right), another report displays information about how employees moved between different zones in the building.

Purposes. Juniper explains that its location tracking system can be used to “understand the movement of people for safety and marketing purposes”.¹⁴⁴ Office facility managers can use it to “optimize space utilization by tracking employee traffic patterns and resource usage”. Retailers can use it to improve “loss prevention”, “optimize shelf management” and to “track personnel and equipment”. Hospitals can use it to “minimize disruptions and delays” and to “monitor personnel for employee health and safety”. Manufacturers can use it “optimize workflows” and to “monitor the precise location of products and equipment like forklifts, pallets, and robotic carts”. Generally, Juniper states that it “provides tailored workflow applications to get the most value out of” its location tracking system and “enable data-driven decision making”, together with its “extensive group of third-party partners”.¹⁴⁵

¹⁴² <https://www.juniper.net/us/en/products/cloud-services/juniper-mist-asset-visibility-datasheet.html> [2.10.2023]

¹⁴³ Figures © Juniper. The figures serve as basis for the discussion of the corporate practices examined in this study. Sources: <https://www.juniper.net/us/en/products/cloud-services/asset-visibility.html>, <https://www.mist.com/documentation/location-dashboards/> [29.9.2023]

¹⁴⁴ <https://www.juniper.net/us/en/solutions/indoor-location.html> [2.10.2023]

¹⁴⁵ <https://www.juniper.net/us/en/products/cloud-services/juniper-mist-asset-visibility-datasheet.html> [2.10.2023]

List of figures

Figure 1: Desk and room occupancy monitoring (Spacewell)	10
Figure 2: Monitoring desk, room and parking occupancy (Spacewell)	12
Figure 3: Monitoring desk occupancy for teams, entry and leave hours, time spent at office (Locatee)	14
Figure 4: Monitoring office and restroom utilization (EnOcean/Aruba), protest against desk monitoring	16
Figure 5: Indoor location tracking map and analysis of device proximity across named employees (Cisco)	18
Figure 6: Indoor location tracking reports and behavioral profiling (Cisco)	19
Figure 7: Accessing current and past locations of devices, searching for devices (Cisco)	20
Figure 8: Indoor location tracking map and reports about employee behavior (Juniper)	24

References

- Christl, Wolfie (2021): Digitale Überwachung und Kontrolle am Arbeitsplatz. Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management? Eine Studie von Cracked Labs, 2021. Online:
https://crackedlabs.org/dl/CrackedLabs_Christl_UeberwachungKontrolleArbeitsplatz.pdf
- Curran, Kevin; Furey, Eoghan; Lunney, Tom; Santos, Jose; Woods, Derek; McCaughey, Aiden (2011): An evaluation of indoor location determination technologies, Journal of Location Based Services, 5:2, 61-78, DOI:
10.1080/17489725.2011.562927
- Kriz, Pavel; Maly, Filip; Tomáš, Kozel (2016): Improving Indoor Localization Using Bluetooth Low Energy Beacons. Mobile Information Systems. 2016. 1-11. DOI: 10.1155/2016/2083094
- Thiede, Sebastian; Sullivan, Brendan; Damgrave, Roy; Lutters, Eric (2021): Real-time locating systems (RTLS) in future factories: technology review, morphology and application potentials. Procedia CIRP. 104. 671-676. DOI:
10.1016/j.procir.2021.11.113